QuickFile

Administration Guide

Version 1.0

QuickFile

Administration Guide

Version 1.0

Note
Before using this information and the product it supports, read the information in "Notices" on page 71.

This edition applies to version 1.0 of IBM QuickFile (product number 5725-F81) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Deploy IBM QuickFile as a virtual appliance

If you are deploying IBM® QuickFile, read the installation and configuration topics before beginning the deployment process.

IBM QuickFile is deployed as a virtual appliance. The advantage of using this approach includes the ease of distributing, installing, and configuring the system. After deployment, you have a virtual machine that can be powered on and used to host QuickFile. A database is required to use the product. The default database is Derby and it requires no special configuration. You can also use IBM DB2 or Oracle.

If you are using QuickFile in a hosted environment, no deployment requirement exists. A hosted environment is also referred to as software as a server (SaaS).

Preparing to use the IBM DB2 database

You can use the DB2 database in place of the default database when you deployQuickFile. To use DB2, you create a temporary table space. Then, deploy the software, run the scripts, and create the properties file.

To configure the DB2 database for use with QuickFile, complete the following tasks in the DB2 instance:

- Create a 32-KB system temporary table space
- Create a 32-KB system buffer pool
- Create 16-KB buffer pool
- Create a 16-KB table space

To configure QuickFile to use DB2, complete the following tasks after you deploy the product:

1. Download the database scripts from the following site: IBM QuickFile Database Scripts.
2. Run the following scripts, in the order that is listed in the following table:

Script	Description
`0_createSchemaObjects.sql`	Creates tables, indexes, and constraints.
`1_loadDefaultSystemData.sql`	Loads system data records.
`2_loadDefaultGroupsAndUsers.sql`	Loads group and user support data records.
`3_loadDefaultConfigurationData_ova.sql`	Loads configuration data records.

3. Customize the properties file to specify that DB2 is being used as the database. See “Customizing the deployment with a properties file” on page 2 for instructions.
4. Deploy the product. See “Deploying QuickFile as a virtual appliance” on page 5.

Tip: If you do not want to use this database, run the script called **`9_dropSchemaObjects.sql`**. It removes all tables, indexes, and QuickFile data. Be sure that you do not need the data before you run this script.

Preparing to use the Oracle database

You can use Oracle as the database in place of the default database when you deploy QuickFile. To use Oracle, enable the use of special permissions, run the database scripts, and customize the properties files.

To configure Oracle to use special permissions with QuickFile, run the following commands as user SYS. Replace <*myOracleUserId*> with the user ID for the Oracle connection.

- grant select on pending_trans$ to <*myOracleUserId*>;
- grant select on pending_trans$ to <*myOracleUserId*>;
- grant select on dba_2pc_pending to <*myOracleUserId*>;
- grant execute on dbms_xa to <*myOracleUserId*>;
- To configure QuickFile to use the Oracle database, complete the following tasks after you deploy the product:
  1. Download the database scripts from the following site: IBM QuickFile Database Scripts.
  2. Run the following scripts, in the order that is listed in the following table:

Script	Description
`0_createSchemaObjects.sql`	Creates tables, indexes, and constraints.
`1_loadDefaultSystemData.sql`	Loads system data records.
`2_loadDefaultGroupsAndUsers.sql`	Loads group and user support data records.
`3_loadDefaultConfigurationData_ova.sql`	Loads configuration data records.

  3. Customize the properties file to specify that Oracle is being used as the database. See "Customizing the deployment with a properties file" for instructions.

Tip: If you determine that you do not want to use this database, run the script called **`9_dropSchemaObjects.sql`**. It removes all tables, indexes, and QuickFile data. Be sure that you do not need the data before you run this script.

Customizing the deployment with a properties file

When you are configuring QuickFile, you can upload a properties file. It enables a DB2 or Oracle database in place of the default database and configure QuickFile to use an external NFS file system.

A properties file can also be used to configure a mail server, change the time zone, or configure LDAP in QuickFile. You can create more than one properties file to define more than one configuration. To customize a function, change the values of the appropriate properties and save the file.

The properties file must have the following characteristics:

- A text-only file with no hidden return or other characters
- Stored in a location where the computer where you deploy the appliance can access it
- UTF-8 encoded
- Accessible for FTP, SCP, or HTTP

You specify the location of a properties file during deployment, in response to the question:

```
Would you like to upload an IBM QuickFile configuration properties file? (y/n):
```

To change the settings on an existing configuration, upload a new version of the properties file and restart the application.

Important: Any line that begins with # is treated as a comment.

The following table identifies the configuration properties:

Section	Property	Description	Requires restart
Mail Server	**smtp.server**	Host name or IP address for the SMTP server.	yes
	smtp.port	Port number of the SMTP server.	yes
	smtp.user	SMTP user name.	yes
	smtp.password	SMTP password.	yes
	smtp.secure.mode	Security mode of the SMTP sessions. Valid values are SSL, TLS, or leave blank for unencrypted sessions.	yes
Hostname	**external.server.host**	External host name or IP address of the appliance. Used with load balancers or VMware proxies.	no
	external.server.port	External port of the appliance. Used with load balancers or VMware proxies.	no
	external.server.port.ssl	External SSL port of the appliance. Used with load balancers or VMware proxies.	no
Domain Name Servers	**dns.servers**	IP addresses for the DNS servers. Multiple addresses are semicolon delimited.	no
NTP Server Addresses	**ntp.servers**	IP addresses of NTP server. Only one NTP server is supported. **Important:** Specify the same NTP server that is used by the underlying hypervisor.	no
Date and Time	**timezone**	Time zone of the current appliance. The appliance and the database must be set to the same value.	yes
NFS	**nfs.server**	Host name or IP address for the NFS server. **Important:** Do not change an existing local file system implementation to an NFS implementation.	yes
	nfs.directory	Directory path that is exported from remote system to be mounted as a file system on the appliance.	yes
	nfs.reset	If set to `true`, unmount NFS directory and reset DB fields app.repository.dir, app.photos.dir, app.email.template.dir to the local system defaults. If set to `false`, causes the exported directory to be NFS mounted.	yes

Section	Property	Description	Requires restart
DB	**db.type**	Database type (DB2 or Oracle). If you use the default Derby database, no database type is required. The application defaults to Derby, unless you define this value.	yes
	db.userid	DB login user ID credentials.	yes
	db.password	DB login credentials - password.	yes
	db.db2.server	DB2 only. Host name or IP address for the database server.	yes
	db.db2.port	DB2 only. Port number for the database server.	yes
	db.db2.name	DB2 only. Database name.	yes
	db.db2.schema	DB2 only. Schema.	yes
	db.oracle.url	Oracle only. Connection URL string	yes
LDAP	**ldap.enabled**	true = LDAP enabled; false = LDAP disabled.	no
	ldap.server.host	The host name or IP address of the LDAP server. Text field. Required (no default).	no
	ldap.server.port	The port number of the LDAP server. Numeric text field. Default = 636. Valid values 1 - 65535.	no
	ldap.user.base.dn	Parent node where users are stored in the LDAP server. Text field. Required (no default).	no
	ldap.group.base.dn	Parent node where groups are stored in the LDAP server. Text field. Required (no default).	no
	ldap.user.search.filter	Search filter for users. Text field. Default is `(|(objectClass=user)(objectClass=person)(objectClass=inetOrgPerson)(objectClass=organizationalPerson))`	no
	ldap.group.search.filter	Search filter for groups. Text field. Default is `(|(objectClass=group)(objectClass=groupOfNames)(objectClass=groupOfUniqueNames))`	no
	ldap.protocol	SSL protocol. Required. Valid values: `ldap` to create a clear connection to the LDAP server, `ldaps` to create an SSL connection to the LDAP server.	no
	ldap.member.attribute	String representing an array of attribute names. Each string specifies the name of an attribute denoting group membership.	no
	ldap.service.principal	Fully qualified distinguished name of an LDAP user who can search the directory. Text field. Required (no default).	no

Section	Property	Description	Requires restart
	ldap.service.principal.password	Password of the service principal. Text field. Required (no default).	no
	ldap.authorized.groups	String representing an array of strings. Each string specifies the DN of an LDAP group that contains users who are authorized to access the QuickFile system. For example: `["cn=Testers,ou=User Groups,ou=QFad,DC=AIXTST,DC=LDAP"]`	no
	ldap.email.attribute	String representing an array of attribute names. Each string specifies the name of an attribute in a user class that identifies an email address. Required. The default value is `["mail","userPrincipalName", "email","emailAddress"]`.	no
System Administrator	**sys.admin.email**	Email address of the system administrator.	no
Application Sender	**app.sender.email**	The "no-reply" account email address. This email address is used for email notifications that are sent by QuickFile.	no

Sample properties file

The following sample properties file specifies the location of an NFS file system and the location of a DB2 database. Oracle database information is commented out. Define your properties file with the values appropriate to your deployment.

```
nfs.server=myserver.example.org
nfs.directory=/localhome/bsmith/NFSdatadirectory
nfs.reset=false

db.type=DB2
db.userid=bsmith
db.password=password
db.db2.server=myDB2server.example.org
db.db2.port=50001
db.db2.name=QUICKFILE
db.db2.schema=QUICKFILE

#db.type=Oracle
#db.userid=cjones
#db.password=password2
#db.oracle.url=jdbc:oracle:thin:@myOracleDBserver.example.org:1522/DEV11R1
```

To specify an NFS server, make sure to remove the # at the beginning of each line in the first paragraph. Specify your NFS server name along with the directory where the NFS data is to be stored. If you do not want to specify an NFS server, comment out these lines.

To specify an Oracle database, comment out the DB2 lines. Then, uncomment the lines for the Oracle database, and provide the values that pertain to your Oracle database.

Deploying QuickFile as a virtual appliance

Use this information to deployQuickFile.

Before you begin

To simplify deployment and administration, QuickFile is delivered as a virtual appliance and is deployed to VMware vSphere Hypervisor (ESXi). Before deploying QuickFile, install an ESXi hypervisor. ESXi is a bare-metal hypervisor that runs directly on hardware. The VMware Compatibility Guide lists the supported hardware platforms for ESXi. Be sure that the vSphere version you use for deployment matches the ESXi version.

Important: Ensure that your hypervisor is configured to run an NTP server.

To deploy a virtual appliance, you need the VMware vSphere client. The client connects to a hypervisor or group of hypervisors, managed by a virtual center. Go to the VMware website and download the VMware vSphere client. Follow the instructions on the website to install the client.

Restriction: ESXi datastores must support at least 2 TB of storage. The minimum disk space that is required for the ESXi host is 100 GB. If the datastores do not support 2 TB of storage with an internal deployment (no NFS), there is a risk of oversubscription with VMware. You must for ensure QuickFile does not exceed the capacity of your datastore.

To deploy a 2-TB virtual appliance, the block size of the datastore must be able to support 2 TB, even with thin-provisioning. To change the block size, delete the datastore and create a new one. The following block sizes are required:

- For ESXi 5.0 and 5.1 with a `VMFS5` datastore, the block size is 1 MB
- For ESX/ESXi 4.1 and ESXi 5.*x* with a `VMFS3` datastore, the block size is 8 MB.

Important: The following ports are open on a QuickFile virtual appliance:

Protocol	Port
WebSphere® MQ	1414
HTTP	9080
HTTPS	9443 - This port is only open if SSL is enabled.

About this task

After you install the VMware vSphere client, complete the following procedure to begin your deployment:

Procedure

1. Gather the following information:
   - The IP address to use for the appliance
   - If wanted, the fully qualified host name to use for the appliance

     CAUTION:
     If you specify a host name, it must be registered with your DNS server. Registering the host name allows the remote clients and the appliance to resolve the host name.
   - IP address of your gateway
   - IP address of your DNS server

- Subnet mask in CIDR format (for example, 24 is the CIDR format for the subnet 255.255.255.0)
- IP address of your NTP server. You must specify the same NTP server that is used by the underlying hypervisor.
- Time zone in POSIX format (for example, `EST5EDT` is US Eastern Time in POSIX format)
- SMTP server name or IP address of the server to use to send email notifications. The email notifications alert users when files are sent or received.
- Password to use to administer the appliance

2. Download the archive named **`QuickFile-1.0.zip`**.
3. Extract the archive. The file named **`QuickFile-1.0.ova`** is extracted. This file contains the QuickFile appliance.
4. Start the ESXi server.
5. To connect to the hypervisor or vCenter, complete the following steps:
   a. Start the VMware vSphere client
   b. Type the host IP address
   c. Type a user name with full access rights and the password
   d. Click **Login**.
6. Choose **File** > **Deploy OVF Template** from the main menu of the vSphere client.
7. When prompted, type the location of the file you extracted.
8. Click **Next** and accept the defaults on the next several pages with the following exceptions:
   - On the Disk Format page, select **Thin Provisioning**
   - On the last page, check **Power on after deployment** and click **Finish**.
9. Wait for the deployment and power on to complete. The process takes several minutes. The OVA file is deployed.
10. Using the vSphere client, go to the **Console** tab to see the QuickFile command line. On this command line, a login prompt is displayed. If not, press Enter.
11. When you are prompted for the login, type `admin` for the user name and `admin` for the password. When you are prompted, provide information that you gathered in step 1 in the following fields.
    - IP address to use for the appliance
    - Subnet mask for the appliance
    - Default gateway for the appliance
12. Confirm the values that you entered.
13. When prompted to set the DNS server, type `Y`, type the DNS server IP address. To specify multiple DNS servers, separate each IP address with a space. Confirm your entry.
14. To change the database to DB2® or Oracle or to specify an NFS file system, upload a properties file. To customize either of these variables, type `Y`. See “Customizing the deployment with a properties file” on page 2. Otherwise, type `N`.

    When you provide all information, the appliance configures itself. This process takes several minutes. A message is displayed, that the application is available at `http://`*`ip address`*`:9080/quickfile/login.html`. Wait a few minutes before you use the appliance.

15. When prompted to change the administrator password, type the new password.

    Tip: To protect the system from external access, define a strong password.
16. Start a web browser and type `http://ip address:9080/quickfile/login.html`
17. Log in to QuickFile as the administrator.

    Important: The default administrator name is `admin` and the password is `admin`. If you changed the password in a previous step, type the new password in this field.
18. Access the Appliance administrative setup pages by clicking **Configuration** from the menu.
19. If you are using the default database, set your time zone on the **Locale** tab. Click **Save**.
20. Add your SMTP server name in the Mail Server section on the **Network** tab and click **Save**. You are prompted to restart the appliance.

    Note: Configuring an SMTP server or changing the time zone requires that you restart your system.
    CAUTION:
    Do not manipulate the database outside the application. Manipulating the database outside QuickFile threatens the integrity and security of product data.

Branding the product to display company information

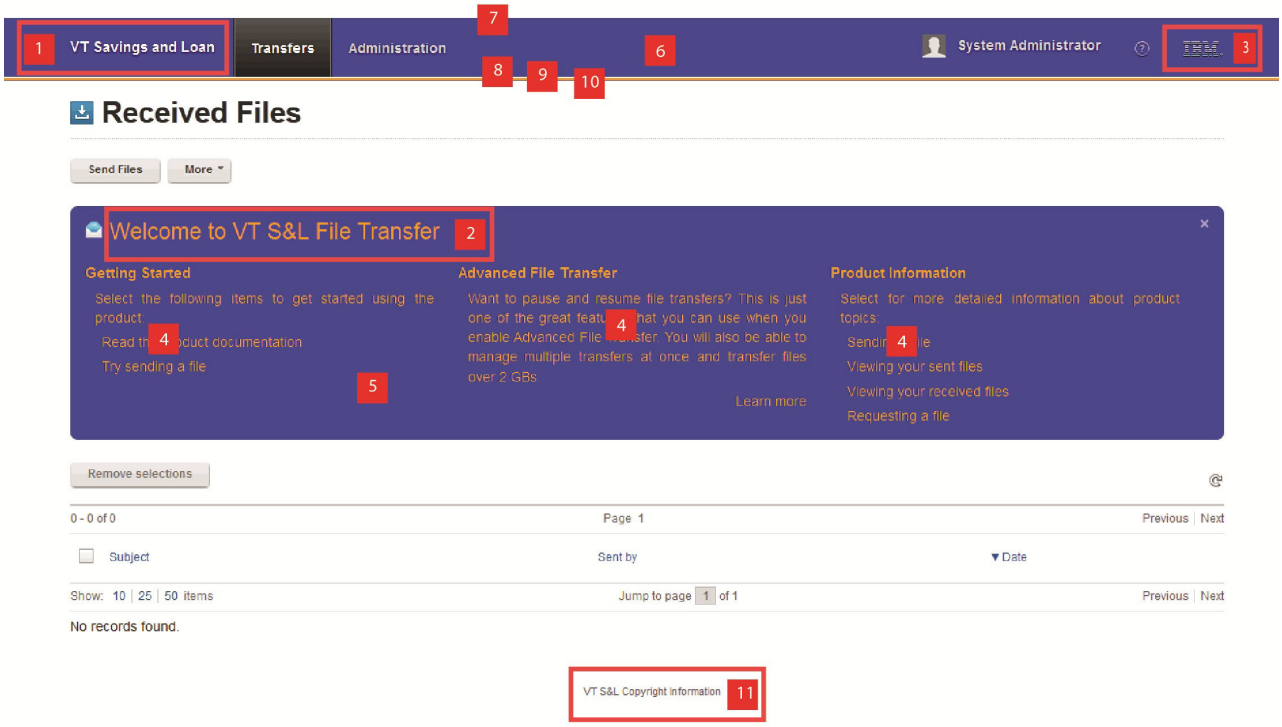
You can customize QuickFile to display your company information on QuickFile pages and email notifications. You can customize the company name, welcome message, colors, logo, and trademark statement.

Complete the following steps to customize each QuickFile page and email notification to display your company information:

1. Create a text file that is called `ui-branding_en_US.properties` and add the following properties:

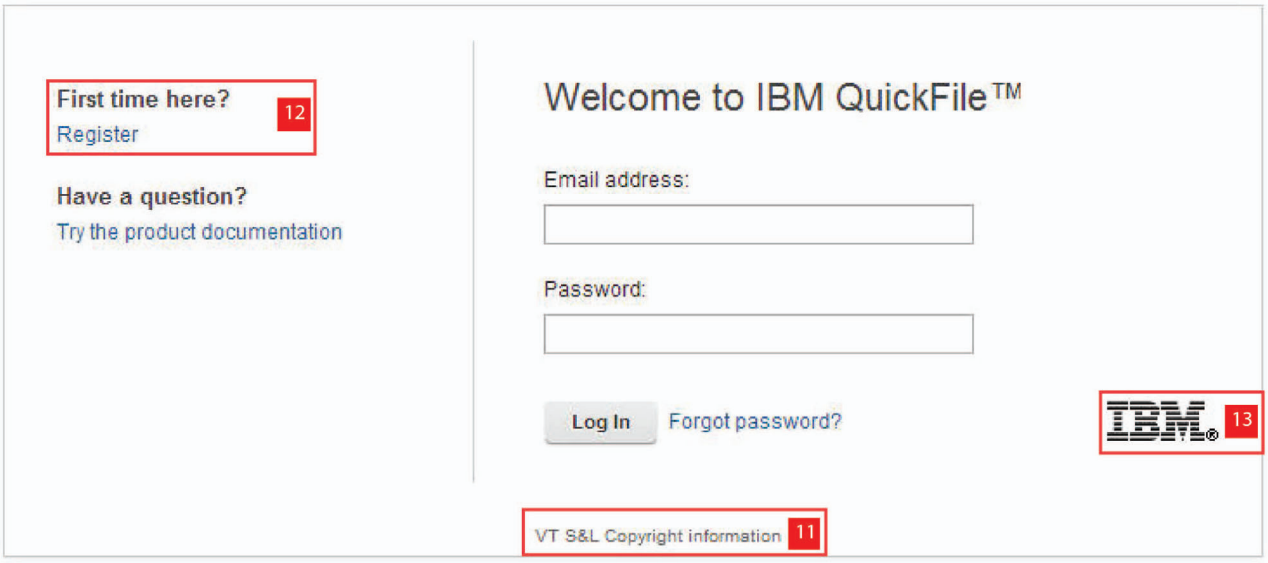
   Tip: If you do not want to customize a property, set the property value to empty. For example, to use the default color for the Welcome divider color, set **`welcomeDividerColor=`**. The default value, black, is used.

   Tip: To remove all branding from the page, set all values in `ui-branding_en_US.properties` to empty.



Property	Valid Values
1 **productLongName**	Full name of the product to display in the interface, for example, IBM QuickFile.
12 **showRegistration**	Determines whether the registration link is displayed on the login page. Valid values are true to display the registration link or false to remove the registration link from the login page. Type the value for this field, true, or false, in lowercase characters.
2 **welcomeMessage**	Welcome message that is displayed on the login page and Welcome banner, for example, Welcome to VT S&L File Transfer.
3 **bannerLogoImage**	Graphic that displays in the banner on each page. The banner logo image can be up to 60 pixels high and 300 pixels wide. Specify the name of the graphic file for this value. Graphic file types can be .jpg, .gif, or .png.
13 **welcomeLogoImage**	Graphic to display as the company logo. The welcome logo image can be up to 60 pixels high and 200 pixels wide. Specify the name of the graphic file for this value. Graphic file types can be .jpg, .gif, or .png.
4 **welcomeDividerTextColor**	Color of the text on the Welcome banner and initially displayed on the Transfers listing page. Use either a hex value, such as #ED7818 or a color name, such as green.
5 **welcomeDividerColor**	The background color on either the Welcome banner or the page divider that is displayed on the file listings page. Use either a hex value, such as #ED7818 or a color name, such as green.
6 **mainBannerColor**	Color that is used on the banner. Use either a hex value, such as #ED7818 or a color name, such as green.
7 **mainBannerTopBorderColor**	Color that is used on the top border of the banner. Use either a hex value, such as #ED7818 or a color name, such as green.
8 **mainBannerBottomBorderColor**	Color that is used on the bottom border of the banner. Use either a hex value, such as #ED7818 or a color name, such as green.

Property	Valid Values
9 **subBannerColor**	Color that is used on the sub banner, the small banner under the main banner. Use either a hex value, such as #ED7818 or a color name, such as green.
10 **subBannerBottomBorderColor**	Color that is used on the bottom border of the small banner that is displayed under the main banner. Use either a hex value, such as #ED7818 or a color name, such as green.
11 **copyright**	Text to display in the copyright property, for example, (C) COPYRIGHT Zeta Hospital 2012. This text appears on every page of the interface including the Welcome page.



2. To brand the email notifications with your company information, create a text file that is called `email_defaults_en_US.properties` and add the following properties:

   Tip: To use the default value for a property, set the value to empty. For example, to use the default color for the company name, set **companyNameColor=**. The default value, black, is used.

   Tip: To remove all branding from the email notifications, set all values in `email_defaults_en_US.properties` to empty.

Property	Description
companyName	Company name to display in the email notification The default value is IBM QuickFile.
companyLogo	Graphic file, in jpeg format, to display above the topic of the email. The default value is `company.jpeg`. The maximum size that is allowed is 25K.
companyNameColor	Font color to use for the company name. Specify colors as HTML color codes, such as #E01B6A, or as a color name, such as blue.
emailTitle	The title on all email notifications.
iHeight	Height dimension for the company logo. The value is defined in pixels.

Property	Description
`iWidth`	Width dimension for the company logo. The value is defined in pixels.

3. Log in to QuickFile as an administrator.
4. From the QuickFile **Welcome** page, click **Send Files**.
5. In the **Send to** field, type a recipient name. Use the format: `username@domainname`, for example `john.doe@company.com`.

   Note: The recipient name is not used. The files are sent to an internal location when you type branding as the Subject value.
6. In the **Subject** field, type branding.
7. Select the `.properties` files that you created and any graphic files to use for the welcome page, banner logo, and company logo.
8. Click **Send**. The files that you created and logo graphic files are sent to the server and define the product pages and email notification branding.

Tip: Once the `.properties` files and logo graphic files are sent to the server, the customization changes are in effect. You do not need to close your browser and reopen it.

Plan your deployment

A critical decision during the planning phase of your deployment is the type of file system. Plan either a local file system or an NFS implementation. You cannot change from one type of file system to the other after deployment. You must start a new deployment.

During the planning phase of your deployment, you must choose between the following file system types:

- Local file system
- Network file system (NFS)

The type of file system cannot be changed after deployment without risk of files that are not retrievable or removable.

For high availability, an NFS server for file storage that both instances share is required.

Understand high availability

High availability is a configuration of two QuickFile instances behind a load balancer.

High availability consists of two QuickFile instances that are controlled by a load balancer. The load balancer is a computer networking methodology to distribute workload across multiple computers. This methodology achieves optimal resource utilization and maximizes throughput. The load balancing service is usually provided by dedicated software or hardware, such as a multilayer switch or a Domain Name System server. QuickFile supports an active / passive high availability configuration. When you configure the load balancer, one instance is configured as the primary instance (active) and one is configured as the secondary instance (passive). The primary is weighted more heavily so it accepts all the traffic unless marked inactive by the load balancer.

Note: QuickFile does not support sticky sessions or session persistence settings.

When you configure the two instances, make sure that the timezone set in both instances matches the timezone that is set for the database. Refer to "Deploying QuickFile as a virtual appliance" on page 5

Configure the load balancer and identify the primary and secondary instances. In a production environment, the primary instance sends and receives files. If the primary instance is unavailable, the load balancer automatically switches work to the secondary instance.

Specific behaviors occur as a result of the switch from a primary to a secondary instance.

- If you use the Advanced File Transfer feature, the high availability instances respond in the following way:
  - If the primary instance loses its connection, the file transfer is interrupted. The transfer is available on the secondary instance and displays as paused on that instance. You can resume the file transfer from the secondary instance after you log in.
  - If the primary instance becomes available while the transfer on the secondary instance is in progress, it is interrupted. The status of the transfer on the primary instance displays as paused. After the user logs in, the user can resume the transfer.
- If you use basic file transfer, the instances respond in the following way:
  - If the user sends a transfer and the primary instance loses its connection before the transfer is complete, the primary instance is not available. The user must log in to the secondary instance and resend the file transfer.
  - If the primary instance becomes available, the file transfer that started on the secondary instance completes. The user must restart the primary instance and log in to use it.

Configuring QuickFile for high availability

Use the information to configure high availability for QuickFile. High availability is two or more QuickFile appliances that share an external database and NFS file system, behind a load balancer. Deploy two OVA files. Then, configure both instances for high availability.

Before you begin

To configure high availability for QuickFile, both instances must be configured with the same information, identified in the following list:

- An external database that both QuickFile instances share
- An NFS server for file storage that both instances share
- Configured for the same timezone that is defined in the database
- The external IP address and port of the load balancer

The load balancer routes traffic to the primary node. If the primary node goes down, the load balancer switches to the secondary node and routes traffic to it. When the load balancer detects that the primary node is back up, it routes traffic back to the primary node. Use the same properties file for each deployment.

Important: When you make configuration changes to QuickFile, you must log on directly to each instance. Do not log on through the load balancer. The same changes must be made to both instances

About this task

Complete the following procedure to set up QuickFile instances for high availability:

Procedure

1. Download the OVA file.
2. Download the database scripts for the OVA.
3. Use database client software, such as dbWiz or Squirrel, to run scripts 0, 1, 2, and 3. The scripts create the database tables and load the default data.
4. On a system that the OVA can access, create a properties file with the configuration of your database instance. Include the NFS configuration and the external IP address and port that is used in the load balancer configuration.
5. Deploy the OVA.
6. Log in to the appliance.
7. Type **Y** to set up the IP address.
8. Type **Y** to set up the DNS.
9. Type **Y** to import the properties file you created.
10. If wanted, change the admin password. This password applies only to this instance. You must change the password of the second instance to keep the two locations in sync.

Results

The configuration takes a few minutes. Then, QuickFile is available.

Upgrading QuickFile as a virtual appliance

Use the information to upgrade QuickFile. If you are using QuickFile in a hosted (SaaS) environment, you are not required to upgrade the appliance. If you are deploying the appliance, you must upgrade the product whenever a new version is released.

Before you begin

Download the upgrade file from the IBM Fix Central website: http://www-933.ibm.com/support/fixcentral/. Enter QuickFile into Product Search. Copy the upgrade file to a server that is accessible from QuickFile. To be accessible, the upgrade file is on a system that the QuickFile instance can access and available using FTP, SCP, or HTTP.

About this task

To upgrade a virtual appliance, use the VMware infrastructure client to connect to a hypervisor or group of hypervisors (managed by a virtual center).

Complete the following procedure to upgrade your deployment.

Procedure

1. Run the following command from your QuickFile console to retrieve the upgrade file from your server:

Command name	Variable Description	Examples

`file get URL filename`	• *URL* is the server path and file name for the upgrade
	• *filename* is the name to save the file as.
		FTP
		`file get ftp://user1@dallas.ibm.com:/downloads/upgrade/091112.vcrypt2 fw`
		SCP:
		`file get scp://user1@dallas.ibm.com:/downloads/upgrade/091112.vcrypt2 fw`
		HTTP:
		`file get http://user1@dallas.ibm.com:/downloads/upgrade/091112.vcrypt2 fw`

   Attention: If you turn off the appliance, the upgrade file is deleted. Upgrade the appliance before you turn off the appliance.

2. After you retrieve the file, run the following command from your console to upgrade:QuickFile

Command name	Variable Description	Example
`firmware upgrade filename`	• *filename* - the name that is used in the file get command.	`firmware upgrade fw`

3. When the appliance restarts, log in to the console.
4. Follow the prompts to complete the startup process. To use the current settings, type `N` when you are prompted to modify properties. To accept a property that changed in the properties file, type `Y`. See "Customizing the deployment with a properties file" on page 2 for instructions on changing properties.

Chapter 2. Administration questions

As administrator, you are responsible for many tasks. Tasks include adding users and groups, configuring security for users, and defining when files are purged from the server.

Use the following table to answer questions you have about administrative tasks:

Question	Answer
How do I make sure that my server has disk space available to add more files?	To make sure that your server has the space available to upload files for transferring, define a schedule for purging files. You define the conditions under which files are removed from the server, including files that are abandoned during upload. Click **Administration** from the menu and select **Policies**. Click the **Schedule** tab to set when files are deleted from the system.
Can I change how many times a user can attempt a login before the user is locked out?	Yes. You can change how many times a user can log in incorrectly before the user is locked out. Click **Administration** from the menu and select **Policies**. Click the **Password** tab to set password options.
Can I control what policies are required for user passwords?	Yes, you can set the strength requirements, how long a password is valid, how frequently a password can be changed, and the characters required. Click **Administration** from the menu and select **Policies**. Click the **Password** tab to set password options.
Can I configure the product to work with Sterling Secure Proxy?	Yes. This product works behind Sterling Secure Proxy. In order for the two products to work together, configure the network configuration to support Sterling Secure Proxy. See "Protecting QuickFile with Sterling Secure Proxy" on page 43
Can anyone decrypt the appliance disk?	No. Direct access to the virtual disk in the appliance is not available. Decryption of the content is not possible.
Can I use the CMIS PI to extract a file that belongs to someone else?	Yes. You can use the CMIS API to extract files. You might want to use the CMIS API to archive files if you do not use FileNet.
When are files archived?	If you configured archiving, files are queued for archiving after the file is uploaded. Files queued for archiving are processed on a first in first out basis.
Are files deleted after they are archived?	No. A copy of the file is moved to the archive queue. The original file is processed by QuickFile. If you configure the purge maintenance task, the files are deleted on the defined schedule.
If NFS is not encrypted, is the environment no longer secure?	Correct. To maintain a secure environment, encrypt the NFS hardware.

Question	Answer
Can I change the default user name and password that is used to connect to WebSphere MQ?	You cannot change the default user name and password.
Can I set up File Download Notification to remove the register link?	Yes. If you configure the file transfer policy and restrict users from inviting other users to register, the registration option is removed from the login page. See • "Setting a policy to define file transfer restrictions and how long an unregistered user invitation and file request are valid" on page 28 • "Defining users who are allowed to send registration invitations" on page 29
How many times can a user download a file?	A user can download a file as many times as needed until the file download expires. "Defining file transfer policies" on page 23

Chapter 3. Setting system management policies

System management policies determine how files are managed system wide by QuickFile.

About this task

As administrator, you can set the system management policies and identify how often to run tasks, manage existing tasks, and create new tasks. Existing tasks include the default expiration of files sent. It also includes if users can override the expiration, or download a file more than one time.

To set system management policies:

Procedure

1. Click **Administration** from the navigation menu.
2. Select **Policies** from the menu.
3. Click the **System Management** tab.
4. To manage the system task schedule, click **Task Scheduler** to display the list of scheduled tasks. See File management field definitions for detailed descriptions of the scheduled task fields.
5. To add a task:
   a. Click **More** > **Add**. The **Add Task** dialog opens.
   b. Give the new task a name.
   c. Select a **Task type** from the list.
   d. Define the interval in which the task is to occur by selecting **Use predefined intervals** or **Use custom intervals** and setting the interval.
   e. Click **Add**.
6. To edit a scheduled task, enable the task name in the **Task Scheduler** list.
7. To suspend a task, check the box next to the task and click **More** > **Suspend**.
8. To resume a suspended task, enable the task and click **More** > **Resume**
9. To manage system file expirations, toggle **File Transfer Expiration** to open the expiration fields. See System management field definitions for descriptions of the file transfer expiration fields.
10. Set **Default expiration for all files sent by users** by selecting a number and the units for the expiration. For example: six weeks.
11. To allow users to override the default expiration period by setting their own expiration date, check **Allow end users to override the default file expiration length**.
12. To allow users to download the same file or package of files more than one time, check **Allow file download multiple times**.
13. Click **Save**.

Chapter 4. Policies that define global user settings

Define policies to identify user settings that affect the way users interface with QuickFile at your installation.

As administrator, you can define policies to set system-wide settings and define how QuickFile works for all users. You can also define groups and apply policies to a set of users with the same requirements.

Note: Not all policies can be applied to a group of users.

Policies include settings for:

- How to manage users who enter incorrect login information
- Define password reset options
- The password strength that is required and how long a password is valid
- When to run common administrative tasks, such as when to clear the database and delete expired transfers
- How to manage file transfer expirations, expiration notices, and email notices
- What users are authorized to send files to internal and external users
- What users can invite users to register
- Limit the size of files that can be uploaded

Account lockout policy overview

As administrator, you can set a policy to define whether users are temporarily blocked from logging in. The policy is enforced after the user fails to log in correctly a defined number of times.

You set how many failed logs in attempts a user can try be the user is locked out. You can define how long the user is locked out.

Setting user lockout policies

Set a temporary user account lockout policy to define when a user is locked out. The lockout occurs after a user attempts to log in multiple times with invalid credentials.

About this task

For security reasons, you can temporarily lock a user out of QuickFile. The lockout occurs if the user fails to provide a valid user ID and password. You define how many tries the user is allowed to provide invalid credentials before the user is locked out. This practice discourages malicious parties from guessing at possible passwords to access an account.

To set the lockout policy:

Procedure

1. Click **Policies**.
2. Click the **Account Lockout** tab.

3. Select **Password lockouts** to enable lockout.
4. Define values in the following fields:
   - **Number of failed login attempts before lockout**
   - **Duration of temporary lockout**
   - **Time before failed login attempt counter resets**
5. Click **Save**.

Account lockout field definitions

To define when a user is locked out of QuickFile after incorrectly entering login information, configure the Account Lockout page. View the following field definitions for information about the Account Lockout page:

Field Name	Description
Password lockouts	Enable or disable password lockout. Optional.
Number of failed login attempts before lockout	How many times the user can unsuccessfully try to log in before the user is locked out. If **Password lockouts** is enabled, select a number 1 - 99.
Duration of temporary lockout	The time that must elapse before the user is allowed to attempt to log in again after the user is locked out. Select a value 1 - 99 and units as minutes or hours for the duration.
Time before failed login attempt counter resets	The time during which failed login attempts are counted, starting with the first failed attempt. The failed attempt counter resets to zero when this time elapses. Select a value 1 - 99 and units as minutes or hours for the time period.

Determine password requirements

As administrator, you can set a policy to define the requirements for a valid password.

You can include one or more of the following password requirements:

- Password strength
- Password complexity definition
- Minimum and maximum duration
- How many passwords in history cannot be used in the password reset
- If a user is allowed to reset a password and how long

Setting a password policy

As administrator, you can define the policies that are used to define the passwords.

About this task

QuickFile provides the method to set policies on secure user access. Password policy settings manage requirements for password strength and duration and set parameters to use to reset passwords.

If your environment uses the lightweight directory access protocol (LDAP) to manage users and passwords, use LDAP to configure QuickFile users. Users who log in using LDAP credentials are managed by LDAP and not by QuickFile policies. Therefore, LDAP users must use LDAP to reset their password. If an LDAP user logs in with an expired password, the user is notified by QuickFile and instructed to contact the LDAP Administrator.

Attention:

Complete the following procedure to set password policies:

Procedure

1. Click **Policies** on the menu.
2. Click the **Password** tab.
3. To set password strength requirements:
   a. If necessary, click **Strength** to display strength options.
   b. Type a value in **Minimum characters in passwords** field.
   c. Define the types of characters users must include in a valid password in the characters options.
   d. If required, type a value in the **Maximum same character allowed consecutively** and **Maximum occurrences of the same character** to define a consecutive character limit and total character limits.
4. Complete the following steps to set how long a password is valid:
   a. Click **Duration**.
   b. Set the minimum change limits, minimum time between password changes, and how many passwords to keep in history.
   a. Set the maximum duration requirements in the password expirations, password expires in. Set the password expiration warning.
5. To set password reset requirements, click **Reset** and set one or more of the following reset requirements:
   a. To allow users to reset their password, enable **Allow users to reset passwords**.
   b. To prevent users from resetting their password, disable **Allow users to reset passwords**.
   c. To set **Time before password reset request expires**, select how many and the units of time.
6. Click **Save**.

Password policy field definitions

Use the following definitions on the **Password Policy** page. Type a zero in a field if you do not want to require that definition in the password.

Field Name	Description
Minimum characters in passwords	Minimum number of characters a password must contain. Range is 6 - 128. The total of lowercase, uppercase, numeric, and special characters that are specified in the following four fields cannot exceed this value. Required.

Field Name	Description
Minimum lowercase characters	Minimum number of lowercase characters the password must contain. Range is 0 - 128. Optional.
Minimum uppercase characters	Minimum number of uppercase characters the password must contain. Range is 0 - 128. Optional.
Minimum numeric characters	Minimum number of numeric characters the password must contain. Range is 0 - 128. Optional.
Minimum special characters	The minimum number of special characters the password must contain. Range is 0 - 128. The following are considered special characters: ~ `! @ # $ % ^ & * ( ) - _ + = { } [ ] | \: ; " ' < >,. ? / Optional.
Maximum same character allowed consecutively	Maximum number of consecutive instances of the same character that is allowed in the password. Range is 0 - 128. Zero indicates no limit on consecutive characters. Optional.
Maximum occurrences of the same character	The maximum number of any character that the password can contain. Range is 0 - 128. Zero indicates no limit on repetitions of a character. Optional.
Minimum change limits	Checking this box sets a minimum time between changes of the user's password and enables password history. Optional.
Minimum time between password changes	Minimum time that must elapse between changes of a user's password. Select the number (1 - 100) and units (minutes, hours, days, weeks, months, years). If **Password expirations** is checked, the value that is specified here cannot exceed the value in **Password expires in**. If **Password expirations** is not checked, the value that is specified here cannot exceed 30 days. Optional.
Number of passwords kept in history	How many former passwords are kept in history. Range is 0 - 99. Optional.
Password expirations	Maximum time that is allowed between password changes. Optional

Field Name	Description
Password expires in	Time within which users must change their password. Select a number 1-365 and units in hours, days, weeks, months, or years.
Warn users before password expires	Generate a warning in advance of the expiration of a user's password (based on the setting in Password expires in). Select 1-30 days.
Allow users to reset passwords	Check this box to allow users to reset their password. Optional.
Time before password reset request expires	Time after which a user request to reset a password expires. When a user clicks **Forget your password?** on the Login page, QuickFile sends the user an access code. The user must click the link in the email and change the password within this time and provide the access code to reset the password. Select a number (1-100) and units (minutes, hours). Optional.

Defining file transfer policies

As administrator you can set system-wide policies that affect when file transfers expire. You can also define whether notifications are sent to users when their files are about to expire. You can set whether users can choose to be notified when they receive files. You can also set a maximum size for individual files that users are allowed to send.

About this task

To set system management policies, complete the following procedure:

Procedure

1. Select **Policies** from the menu.
2. Click the **System Management** tab.
3. To manage file expirations:
   a. Click **Expirations** to expand the section.
   b. Set the default file expiration period by selecting the number and units for **Default expiration for all files sent by system users**.
   c. To let users override the default expiration by setting their own expiration, enable **Allow end users to override the default file expiration length**.
4. To manage when users are notified that file transfers are due to expire:
   a. Click **Expiration Notifications** to expand the section.
   b. Set a final notification by enabling **Send final warning notification before the transfer expires**. Select how long before a file transfer expires the final notification is sent.
   c. Set an initial notification by enabling **Send initial warning notification before the transfer expires**. Select how much time before expiration the initial notification is sent.
   d. To change the frequency of expiration notifications, click **Edit Reminder task schedule**. See Scheduling tasks for information.

5. To set that maximum file size that can be transferred, click **File Size** and type a maximum size in megabytes.
6. Click **Save**.

System management field definitions

Use the System Management page to define when file transfers expire and when users are notified. The following table provides information about the fields on the system management page.

Field Name	Description
Default expiration for all files that are sent by system users is	When files expire and are unavailable to the recipient. The initial default is set to 30 days. Values range from 1 - 100. Set units to hours, days, weeks, months, or years. Required.
Allow users to override the default file expiration length	Allows users to set their own file expiration length. If you check this field, the user can set a default file expiration length. This value can be changed when a file transfer is defined. If this field is not enabled, the user cannot set a personal default or an expiration for a specific file transfer. Optional.
Send final warning notification before the transfer expires	Defines when to send a final warning notification to notify a user that a transfer is expiring. After a file expires, it cannot be downloaded. Define a range from 1 - 100 with units of hours, days, weeks, or months. Optional.
Send initial warning notification before the transfer expires	When to send an initial warning, that a file transfer is expiring soon. After a file expires, it cannot be downloaded. Define a range from 1 - 100 with units of hours, days, weeks, or months. Optional.
Limit the size of individual files that are uploaded to	Set this field to establish a limit for the size of individual files. Values can range from 1 MB to 1 TB. Optional. If the file size exceeds this limit, a system notification event is generated and users are unable to upload the file.

Tasks available to schedule

Configure QuickFile to complete predefined system-wide maintenance tasks on a regular schedule. The list of tasks is defined by QuickFile. You select a task to schedule and define when the task runs. You can start a task manually or set up a schedule when the task runs. You can also suspend a task that is running and resume it later. If you suspend a task, you must manually resume it. The default state for Scrub is Suspended. The default state for all other tasks is Scheduled.

The following table describes the tasks that are scheduled to run. Change the value of each task to prevent the task from running:

Lifecycle Task	Description
Notification	Queues all outstanding email notifications and prepares them to be sent.
Purge	Marks all packages that expired and any incomplete file transfer packages and makes them available for deletion. An incomplete package is one that was sent but was interrupted and did not complete the transfer within seven days. It cannot be downloaded. When a scrub occurs, all packages marked for deletion are removed from the database. **Attention:** Do not run the purge task at the same time that you run scrub. These tasks access the same records and running them at the same time might cause a problem.
Reminder	Queues all outstanding reminder emails and makes them available to send.
Scrub	Removes records that are marked for deletion from the QuickFile database. **Attention:** Do not run the scrub task at the same time that you run purge. These tasks access the same records and running them at the same time might cause a problem.
Status	Batch removal of database records after they are no longer required.
User	Performs maintenance of user and group-related records. Examples include removing registrations that are expiring and identifying expiring SSL certificates.

Define when maintenance tasks occur

As administrator, you can schedule predefined tasks to run regularly. These tasks keep QuickFile running efficiently and meet business requirements.

Configure QuickFile to use predefined maintenance tasks on a regular schedule. The list of tasks is defined by QuickFile. You configure the maintenance tasks to schedule for your environment. You can start a task manually, set up a schedule by which to run a task, and suspend and resume tasks. The default state of Scrub is Suspended. The default state for all other tasks is Scheduled.

QuickFile provides the following methods to set up schedules:

Scheduling Method	Description
Predefined	Use predefined intervals as a simple method to define a schedule. Select one of the following predefined intervals: • Yearly to schedule a task one-time per year at 12:00 a.m. on 1 January • Monthly to run a task on the first day of every month at 12 a.m. • Weekly to run a task every Sunday at 12:00 a.m. • Daily to schedule the task at 12:00 a.m. every day • Hourly to schedule the task at the beginning of every hour
Interval	Options that allow finer control over scheduling. You can run a task every *x* minutes or hours, and every day or every weekday.
Date-Time	Identifies specific days of the week when the task is run. You choose the days of the week and the times to run the task. For example, set a task to run each Tuesday and Thursday at 6:00 a.m. and 6:00 p.m.
CRON	A notation method that uses a limited set of characters in a special syntax to express scheduling times. This application supports CRON notation to define date-time intervals and specifies six terms to define the expression. While other approaches to CRON use five terms, this application requires six terms and does not support five terms. Consult the WebSphere Application Server documentation and search on the topic title: Interface User Calendar. **Important:** Because of the complexity of CRON expressions, QuickFile uses only limited validation of your entries.

Scheduling maintenance tasks

Use the **Schedule** tab under Policies to set schedules to fit your requirements for the tasks QuickFile must complete regularly.

About this task

QuickFile must routinely perform certain tasks, in order for the system to function smoothly. Maintenance tasks are scheduled to run on a default schedule. The task scheduler can set up a custom schedule for each task. You can also suspend or resume a task, or set it to run immediately. This procedure defines the steps to take to define scheduling or to manually run a task. Refer to the Task scheduling overview for information about how to use the scheduler.

Attention: Do not schedule the purge task at the same time that you schedule scrub. These tasks access the same records and running them at the same time might cause a problem.

To manage scheduling:

Procedure

1. Click **Policies** on the menu.
2. Click the **Schedules** tab.
3. By default, only scheduled tasks are displayed in the schedule list. Click **Show all tasks** to view the full set of tasks.
4. To immediately run a task, select the task and click **Run**.
5. To define a custom schedule to use for a task in the list, complete the following steps:
   a. Enable the task and click **Edit**.
   b. Click the tab of the scheduling method to use.
   c. Set up the interval to use to run the task. See for information about the scheduling methods and options.
   d. Click **Save** to save your changes.

What to do next

If you detect that scheduled tasks are not running or are running at unpredictable intervals, and the hypervisor is ESXi5, take the following actions:

- Ensure that the hypervisor NTP server is configured and running.
- Verify that the QuickFile NTP server and underlying hypervisor are using the same NTP server.

Suspending or resuming a task

Use the **Schedule** tab under Policies to suspend a task that is running or to restart a task that was suspended.

About this task

QuickFile must routinely complete certain tasks, in order for the system to function smoothly. After you schedule tasks to run regularly, you can suspend a task and resume it later.

To suspend a task and restart in later, complete the following procedure:

Procedure

1. Click **Policies** on the menu.
2. Click the **Schedules** tab.
3. Enable the task to suspend and click **Suspend**.
4. To restart the task, complete the following steps:
   a. Click **Show all tasks** to view all tasks.
   b. Enable the task to restart and click **Resume**.

Task scheduler field definitions

Define the fields on the **Schedules** tab of Administration Policies to define what tasks are displayed and how often to run the schedule.

Field Name	Definition
Show only scheduled tasks	Click this option to show only tasks with an established schedule. Default.
Show all tasks	Click this option to show all tasks regardless of whether their schedule is defined. Optional.
Name	The name of the task. The tasks in this list are determined by the server and are not editable. Also, tasks cannot be added or removed. Click the task name to edit its schedule. Current valid values for task names are Lifecycle, Notification, Purge, Reminder, Status, and User.
Status	Indicates whether a schedule is set up for the task and whether the task is currently running or suspended. Valid values are Scheduled, Not Scheduled, Running, or Suspended.
Interval	The schedule interval. See the Task scheduler overview topic for information about possible values this field contains. Display only.
Next run	The date and time when the task is next scheduled to run. Expressed as a date (or Today if so scheduled) and a time. Display only.

User management policy overview

As administrator, you can define a user management policy. It identifies what functions a user can perform, including who a user can send files to and who a user can invite to register.

You can set a policy to control what users are allowed to do in QuickFile. These settings determine whether users can send files to internal or external users, and whether users can invite others to register with QuickFile. If you allow users to send invitations to register with QuickFile, you can define when the invitation expires.

Setting a policy to define file transfer restrictions and how long an unregistered user invitation and file request are valid

Define whether users can invite other users to register with QuickFile. In addition, identify who can send a file transfer and what type of user can receive the files.

About this task

Use this procedure to define who can transfer files and who can invite an unregistered user to register. You can also define how long an unregistered user is allowed to register and is allowed to use the email link to send files. When an unregistered user sends files when invited to do so, the files expire five days after they are sent. For example, fred@company.com sends a request to

mary@company2.com to send files. Mary sends file to fred@company.com on October 1, 2013 at 06:00AM. Fred has until October 6, 2013 at 06:00AM to download the files.

Complete the following procedure to view or set user management policies:

Procedure

1. Click **Policies** from the menu.
2. Click the **User Management** tab.
3. To view or set file transfer policies, click **File Transfers** and enable or more of the following policies:
   - To prevent external users from sending files to other external users, select **Only internal users can send files to external users**.
   - To allow any registered user to send files to anyone, select **Internal and external users can send files to anyone**.
4. To set the policies about inviting other users to register, click **Invitation to Register** to display the policies. Select one of the following values to assign to this feature:
   a. To prevent users from inviting others, click **Disallow users to invite others to register**.
   b. To allow only internal users to send invitations, click **Only internal users can invite others to register**.
   c. To allow any registered user to invite others to register, click **Internal and external users can invite others to register**.

Defining users who are allowed to send registration invitations

Define which users can send registration invitations by defining them in the User Management policy. A user who registers is allowed to send and receive files, if the administrator activates permissions. A registered user can also view information about how many file transfers were sent and received.

About this task

The User Management policy identifies:

- Which users can send registration invitations
- Whether internal users can send files to external users
- Whether file transfers can be requested or sent from unregistered users
- How long an unregistered user is allowed to register after the user receives an invitation

To set the User Management policy:

Procedure

1. Click **Policies** from the menu.
2. Click the **User Management** tab.
3. Click **Invitation to Register**.
4. Enable one of the following options
   - To prevent users from sending registration invitations, enable **Disallow users to invite others to register**.

- To allow only internal users to send registration invitations, enable **Only internal users can invite others to register**.
- To allow all users to send registration invitations, enable **Allow users to invite others to register**.

5. Define how many days an invitation is active in the **Invitations to register expire in** field.
6. Click **Save**.

File transfer policy field definitions

The File transfer definition on the **User Management Policies** page defines who can send file transfers to external users.

Field Name	Description
Only internal users can send files to external users	Select this option to allow only internal users the ability to send files to users outside of the company.
Internal and external users can send files to anyone	Select this option to allow both internal and external users to send files to one another. An internal user is defined on the domain within the company. An external user is a user outside of the company server.

Invitation to register policy field definitions

The Invitation to register policy field definitions provide information about the fields you can configure to define who can invite an external user to register.

Field Name	Description
Disallow users to invite others to register	Prevents all users from requesting that another user register.
Only internal users can invite others to register	Allows only internal users to the ability to send a request to register to an external user.
Internal and external user can invite others to register	Allows all users to invite other users to register.

Chapter 5. Managing user accounts

QuickFile makes it easy for an administrator to add new users to the system. In addition to creating new user accounts, you can temporarily lock an account, unlock it, or permanently delete it.

Before you begin

To manage user accounts:

Procedure

1. Click **Administration** from the navigation menu.
2. Click **Users** from the menu. The list of current users is displayed. The columns show the user name, role, group the user is assigned to, user type, and status of the user account.
3. To add a user account:
   a. Click **Create**.
   b. Type the new user **Email address**. Confirm the address in the **Confirm email address** field.
   c. Type the user **Full Name**.
   d. Click **Create**. The user receives a notification email with a link to the temporary access code. The user must click the link in the email and use the temporary access code to complete the setup.
4. To edit an existing profile, click the user name in the list of users. For information about the fields on the **Profile** page, see the User profile field definitions topic in the *QuickFile User Guide*.
5. To prevent a user from logging in to QuickFile, enable the check box next to the user name and click **More** > **Lock**.
6. To unlock a user account, enable the check box next to the user name and click **More** > **Unlock**.
7. To change a user role, enable the check box next to the user name and click **More** > **User role**, then click the appropriate role (Admin or User). Access to the administrative tools in QuickFile is limited to users of type Admin.
8. To change a user authentication type, enable the box next to the user name and click **More** > **Authentication type**, then click the appropriate type (Company LDAP or Application).
9. If you switch the authentication type from LDAP to QuickFile, you receive an email with an access code. Use the access code to reset your password.

   Restriction: This field is active only if you establish a connection between QuickFile and your company lightweight directory access protocol (LDAP) server. For more information, see the User management overview topic.
10. To delete a user, enable the check box next to the user name and click **Delete**. Confirm the deletion by clicking **Delete** again. After a user account is deleted, that user cannot log in again and must register as a new user to use the system. Activity from a deleted account is no longer available.
11. To reset your account, click **More > Reset**.

Functions to define in user accounts

You can add users to QuickFile. You can modify user definitions, including a profile. You can lock a user out of the system, unlock a user, or reset a user who did not register within seven days. You can also identify the authentication method for a user, as LDAP or QuickFile.

You can perform the following functions in a user account:

- "Creating or editing a user account"
- "Deleting a user account"
- "Resetting a user account setup" on page 33
- "Locking or unlocking a user" on page 33
- "Changing a role assigned to a user" on page 33
- "Changing a user account authentication type" on page 34

Creating or editing a user account

Use QuickFile to add a user to the system. After the user is added, the user receives a New User Registration notice. The user must click the link in the email notice and define a password within seven days. If not, the registration expires. You can reset a user account to allow the user more time to register. After you create a user account, you can modify the account and change any of the settings. Access to administrative tools is limited to Admin users.

Before you begin

Complete the following procedure to create a user account:

Procedure

1. Click **Users** from the menu. The list of current users is displayed.

   The columns list the user name, role, groups the user is assigned to, user type, and status of the user account.
2. Click **Create**.
3. Type the user **Email address**. Type the same address in the **Confirm email address** field.
4. Type the user **Full name**.
5. Click **Create**.

What to do next

To edit an existing profile, click the user name in the list of users. For information about the fields on the **Profile** page, see the **User profile** field definitions topic in the *IBM QuickFile User Guide*.

Deleting a user account

You can add a user account or a user account is added when a user registers. Use the **User** page to delete a user account that is no longer needed.

About this task

To delete a user account, complete the following procedure:

Procedure

1. Click **Users** from the menu. The list of current users is displayed.
2. To delete a user, enable the check box next to the user name to modify and click **Delete**.
3. Click **Delete** to confirm the deletion.

   Attention: After a user account is deleted, that user cannot log in again and activity is no longer available. The user must register to use the system.

Resetting a user account setup

When you create a user account, a New User Registration notice is sent to the user. To complete the user account setup, the user must click the link in the notice and define a password. The process must be completed within seven days or the user account setup expires.

Before you begin

If the user setup expires, the administrator can reset the user account. The user is then given seven more days to update the password.

To reset the user account setup:

Procedure

1. Click **Users** from the menu. The list of current users is displayed.
2. Enable the check box next to the user name to reset.
3. Click **More** > **Reset**.

Locking or unlocking a user

Use QuickFile to lock out a user to prevent access to the system. You also can unlock a user that you locked.

Before you begin

To lock a user or unlock a user:

Procedure

1. Click **Users** from the menu. The list of current users is displayed.
2. To prevent a user from logging in to QuickFile, enable the check box next to the user name and click **More** > **Lock**.
3. To unlock a user account, enable the check box next to the user name and click **More** > **Unlock**.

Changing a role assigned to a user

As administrator, you can change the responsibilities that a user is allowed to perform. By default, a user is defined as a basic user. The user can send a file and receive a file but cannot change any policies, environmental settings, or add users. Administrators can perform all of the functions that a user can perform and can also define policies, configure the environment, and add users. Access to administrative tools is limited to Admin users.

Before you begin

Complete the following steps to change a user role:

Procedure

1. Click **Users** from the menu.
2. Enable the check box next to the user to modify.
3. Click **More** > **User role** and select the role to assign to the user: Admin or User.

Changing a user account authentication type

Configure QuickFile to identify how a user is authenticated. Select QuickFile or LDAP to manage user credentials for each user. Users who are authenticated by LDAP are defined by the LDAP server. LDAP users log in to QuickFile with their LDAP credentials. LDAP users are not required to register with QuickFile.

Before you begin

The lightweight directory access protocol (LDAP) is an industry-standard Internet Protocol. It stores and accesses user information from an LDAP server. If your company uses LDAP, you can make that data available to QuickFile.

Restriction: The Company LDAP option is active only if you establish a connection between QuickFile and your LDAP server.

With an LDAP connection, you can define users and user groups with LDAP and eliminate the need to define users in QuickFile.

If you enable LDAP, do not use QuickFile to add and manage user credentials. Use the LDAP tools instead. If a user tries to log in to QuickFile with an expired LDAP password, the user is notified that the password expired. The user or the LDAP administrator must change or reset the password on the LDAP directory. The LDAP directory is created and managed separately from QuickFile.

To change a user authentication type:

Procedure

1. Click **Users** from the menu. The list of current users is displayed.
2. Enable the box next to the user name to edit and click **More** > **Authentication type** and select the authentication type: Company LDAP to use LDAP or Application to use QuickFile.

   Attention: If you switch the authentication type from Company LDAP to QuickFile, the user receives an email with an access code and instructions to set their password in QuickFile.

User account listing fields

The User Account fields listing provides information about the information displayed for each defined user. Use the User Account page to view user information.

Field Name	Description
Name	The full name of the user, as provided when the user account was created, or as edited by the user or administrator. Required.
Role	Type of user. A User is a regular user who can send and receive files but cannot add users or policies. An Admin can add policies, add and modify users, lock and unlock users, delete users, and change configuration settings.
Groups	The QuickFile group to which the user is assigned. The user can only be assigned to 1 group. Admin users cannot be added to a group when you define the user. However, Admin users are added to a default group, if one is defined.
Type	Identifies a user as internal or external. An internal user is defined on the domain within the company. An external user is a user outside of the company server.
Status	The status of the user account. Possible values are: lock, unlock, delete, pending registration, registration expired, or departed. Departed is a user who is removed from LDAP and later, attempts to log back in to the system.

User account field definitions

The User Account field definitions provide information about the fields on the **User Account** page. Use the **User Account** page to create and view user information. You can create a user account or view information about an existing account. You can delete a user account. You can change the account type, the user role, and the authentication method. By clicking the name of a user on this page, you can view and edit information on the user Profile page.

Field Name	Description
Email address	The email address that is used to send and receive files. Specify this value when you create a user through the Create User dialog.
Confirm email address	When you add the user account, retype the email address for verification. Required.
Full name	The full name. Required.

Chapter 6. Use groups to manage user settings

Create a group and add users to the group to quickly assign similar policies to a group of users.

Be sure to define default policies before you define a group. You can then assign the default policies, including file management, password, and lockout policies to the group. Based on the user requirements, you can create a group and define a custom policy for one or more of the policies. A user can be assigned to only one group.

Creating a group

You can quickly define what functions a user can perform by creating a group, associating policies with the group, and adding users to the group. As needed, you can edit and delete groups.

About this task

To create a group and add users and policies to the group:

Procedure

1. Click **Groups** from the navigation pane.
2. To create a group, click **Create**.
3. Type a name and description for the group.
4. To use this group as the default for all newly registered user, click **Make this the default group for newly registered users**.
5. Click **Next**.
6. To use the default policies, enable **Use the default policies for the group**.
7. To set custom settings for one of the following areas, click **Define a custom policy for this group**. Define settings for the policy definition.

Option	Description
Policy to customize	**Link to procedure**
Temporary lockout	"Setting user lockout policies" on page 19
System management policies	"Defining file transfer policies" on page 23
Password policies	"Setting a password policy" on page 20
System management policies	"Defining file transfer policies" on page 23
User management policies	Define who can invite an external user to register and Defining who can send file transfers

8. Click **Next** to move through the wizard.
9. Move a user from the left window to the right window to add the user to the group. Use the procedure Chapter 5, "Managing user accounts," on page 31 to add users to the group.
10. On the **Summary** page, validate that all settings are correct and click **Finish**.

Editing a group

You can modify a group to change information, including users that are assigned to the group and policies that are associated with it.

About this task

To edit a group, complete the following steps:

Procedure

1. Click **Groups** from the navigation pane.
2. To edit an existing group, click the group name from the listing.
3. If wanted, modify the name, description, or if this group is applied to newly registered users.
4. To change the policies that are associated with the group, click the **Policies** tab and modify one or more settings:
   - To modify the lockout policy settings, use the procedure, "Setting user lockout policies" on page 19.
   - To modify the file management policy, use the procedure, "Setting a policy to define file transfer restrictions and how long an unregistered user invitation and file request are valid" on page 28
   - To modify the password policy, use the procedure, "Setting a password policy" on page 20
   - To modify the system management policy, use the procedure, "Defining file transfer policies" on page 23
5. If necessary, click **Members** to add or remove users from the group. Use the procedure Chapter 5, "Managing user accounts," on page 31 for instructions.
6. On the **Summary** page, validate that all settings are correct and click **Save**.

Deleting a group

You can delete groups that you no longer need. You can delete multiple groups at one time.

About this task

To delete a group:

Procedure

1. Click **Groups** from the navigation pane.
2. Select the groups to delete and click **Delete**.
3. Click **Delete** to confirm the deletion.

Groups field definitions

The following table lists the fields on the **Groups** page and their definitions:

Field	Definition
Name	Name that is assigned to the group.
Description	Description of the group.

Field	Definition
Make this group the default group for newly registered users	Select this option to use the defined group settings for any new users who are register with QuickFile.
Define custom policies for this group	Select this option to define new custom policies for the group. You can define settings for one or more policy types.
Policies tab	Click this tab to display the policies that you can define. Refer to "Setting user lockout policies" on page 19 to define a lockout policy, "Setting a password policy" on page 20 to configure a password policy, "Defining file transfer policies" on page 23 to configure a file transfer policy, "Setting a policy to define file transfer restrictions and how long an unregistered user invitation and file request are valid" on page 28 to configure a user policy, and
Members	Select this tab to define the users that are associated with the group. To add users to the group, highlight the users in the left panel and click the right arrow. Users in the right window are members of the group.
Summary	The summary page displays the group definition, including the name and description of the group. It also identifies what policies are custom policies, and how many users are in the group definition.

Chapter 7. Configuration overview

Configuration options are available to control the setup of QuickFile. Many of the setup options are defined when you deploy the product. Use the Configuration options to modify or add new settings.

As needed, change the setup of QuickFile. Change the configuration of the following areas:

- Network - change the basic settings of the network, including the network or DNS address or the host name (fully qualified domain name - FQDN). Check the basic settings after you deploy the product. If you have a firewall that is defined, change the advanced network settings. You can also identify a user on a specific email domain as an internal user.
- Locale - defines the time zone for the server. Use the locale options to change the time zone.
- Power - Shuts down or restarts QuickFile.
- LDAP - use this option to configure LDAP.
- Archiving - enables archiving and configures IBM FileNet®.
- SSL - enables SSL authentication.

When to configure network options

Network options are defined when you deploy the product. View the basic network options after the installation to validate the settings. If necessary, modify the basic network values. For certain network environments, such as the presence of a firewall or the need to identify internal users, configure advanced network settings.

- Use the procedure that is called *Setting basic network configuration options* to validate the network address that is defined for the installation or disable the ethernet connection.
- Use the procedure that is called *Configuring advanced network options* to configure network requirements specific to your environment. Options include adding or removing a DNS server definition or defining the domain where internal users are stored. In addition, define an SMTP mail server, modify the mail server definition, or configure support for a firewall.

Setting basic network configuration options

Network settings are first set up when the product is installed. After you install QuickFile, use this procedure to validate basic network settings and change them as needed.

Before you begin

Perform the following procedure to view and change basic network settings:

Procedure

1. Click **Configuration** from the menu.
2. On the **Network** tab, click **Network Addresses** to display the address options.
3. To modify an Ethernet interface, complete the following steps:

a. Enable **eth0** to enable the Ethernet interface.
b. Type the IP address for the Ethernet interface in the **IP Address** field.
c. Enter the appropriate **Mask** value in CIDR format.
d. Type the **Default gateway** address for the interface.

4. To disable an Ethernet interface, disable the box next to its name.
5. To add a domain name DNS server address, click **Click to add**, type the DNS name, and press Enter.
6. To delete a DNS server, click the **x** beside the server address.
7. To enable the host name that is defined for the network, complete the following steps:
   a. Click **Host Names** to display the host name option.
   b. Type the host name in the **Hostname** field.
8. To configure the NTP server and the time zone for the server, complete the following steps:
   a. Click the **Locale** tab.
   b. To add an NTP server address, click **Click to add** and type a new address.
   c. To delete an NTP server address definition, click the **x** next to its name.
   d. To change the time zone for the server, select the time zone to use, from the list.
9. Click **Save**.

Configuring advanced network options

Configure advanced network settings to prepare specific environments. Set the domains where users are stored in addition to the address set at installation. Configure the email domain name where internal users are stored. Define the public facing network options to configure a firewall.

Before you begin

To view and change network settings for environment requirements, complete the following steps:

Procedure

1. Click **Configuration** from the menu.
2. If necessary, click the **Network** tab.
3. To define the domain where internal users are located, complete the following steps:
   - Click **Mail Domains** to display the mail domain options.
   - To add an **Internal Email Domain**, click **Click to add**.
   - Type the domain name where internal users are stored and press Enter.
4. To change the SMTP mail server, complete the following steps:
   - Click **Mail Servers** to display the mail servers options.
   - Type a server name in the **SMTP Server Name** field and a port in the **SMPT Server Port** field.
   -
   -
   -
5. To enable security, complete the following steps:

a. Select **SSL or Start TLS** from the **Security** field.
b. Add the certificate for the SMTP server to the truststore.

6. To authenticate access to the SMTP server, click **Use authentication credentials with smtp server**, then supply the Authorized user name and Authorized password credentials.
7. To configure the product to support a firewall, complete the following steps:
   - Enable **Use a hostname (fully qualified domain name (FQDN) or IP address** to select the method of connecting to the server.
   - Type the host name to use to connect to QuickFile in the **public-facing Hostname** field.
   - Type the **Port number** for this host name.
8. Click **Save**.

   Note: You cannot change a user from an internal user to an external one. To change a user from an internal user to an external user, delete the user account. Then, ask the user to register again. By default, users are defined as external

Protecting QuickFile with Sterling Secure Proxy

You can use IBM Sterling Secure Proxy to protect QuickFile in the internal network.

Before you begin

Configure an HTTP configuration in Sterling Secure Proxy. See the Sterling Secure Proxy information center for information.

Important: The inbound and outbound HTTP connections can be secure or unsecure, but they must match. If the inbound netmap connection is secure, the outbound netmap connection to QuickFile must also be secure.

Complete the following procedure to configure QuickFile to work with Sterling Secure Proxy:

Procedure

1. Click **Configuration** from the menu.
2. If necessary, click the **Network** tab.
3. To configure the product to support Sterling Secure Proxy, complete the following steps:
   - Type the host name or IP address of the Sterling Secure Proxy HTTP adapter in the public-facing **Hostname** field.
   - Type the **Port number** of the Sterling Secure Proxy HTTP adapter for this host name.
4. Click **Save**.

   Important: If you configured QuickFile to use a self-signed certificate for SSL, you must export the root certificate and use it to configure the Sterling Secure Proxy HTTP netmap. See the Sterling Secure Proxy information center for more information.

Solving network issues

Solve network issues that are identified by users and how each issue was solved:

Table 1. Network issues

Issue	Solution
While a user was testing the appliance, the user incorrectly set up the network. The network had errors so I was unable to log in to correct the problem. Is there a command to reset the appliance so I can correct the setup?	In the console view of the appliance, run the setup wizard again by entering the following command on the command line: **wizard startup.xml** Reset just networking by entering the following command: **netif set eth0 IPAddress=** *youripaddress***DefaultGateway=***yourdefaultgateway*Substitute your IP address for *youripaddress* and your gateway address for *yourdefaultgateway*.

Network configuration field definitions

Define the following fields on the **Network** tab of the Configuration settings to configure basic and advanced network settings:

Field Name	Description
Ethernet interface (eth*x*)	The Ethernet interface that is defined. One Ethernet interface (eth0) is required. Only one Ethernet interface is supported.
IP Address	The IP address or mask of the Ethernet interface. Required.
Mask	The subnet mask for this IP address. It must be in classless inter-domain routing notation. (CIDR), a means of specifying IP addresses and their routing prefix. It provides the decimal number of leading bits of the routing prefix. For example: 24. Required.
Default gateway	The default gateway address for the Ethernet interface. Required.
DNS Server address	The address of the DNS server.
Internal Email Domains	The domain name servers (DNS) for the appliance. At least one domain is required.
SMTP Server Name	The SMTP or mail server to use to route email for the appliance. Required.
SMTP Server Port	The SMTP or mail server port to use to route email. Required.
Security	Security used by the SMTP server: Valid values are None, SSL, or Start TLS.
User authentication credentials with smtp server	Enables the use of authentication credentials with the SMTP server
Authorized username	A user name with authorization to access the SMTP server. Optional.
Authorized password	The password for the user who is authorized to access the SMTP server. Required if **Authorized user name** is specified.

Field Name	Description
Use a hostname (fully qualified domain name - FQDN) for the application	Enable this option only when a host name is assigned to the QuickFile appliance, and the host name to IP address mapping is added to DNS. When this field is enabled, you can access QuickFile by using the fully qualified distinguished name. The distinguished name is easier to remember than an IP address. If you set this field to a host name that cannot be resolved by the appliance DNS, an error occurs.
Hostname	DNS host name of the QuickFile appliance. If no host name is assigned, the field displays the IP address of the first network that is configured.
Use a public facing domain name (FQDN) or IP address	Check this field when QuickFile is deployed behind a reverse proxy or load balancer. If this option is enabled, type the public facing, fully qualified domain name and port to use to access the proxy or load balancer. The proxy or load balancer routes requests that it receives to QuickFile
Public-facing Hostname	If **Use a public facing domain name (FQDN)** is checked, type the proxy or load balancer host name or IP address where client traffic is routed.
Public-facing Port number	Port to use to access the proxy or load balancer. • If you configure a load balancer and SSL, set the port value to 9443. For a non-secure load balancer, define the port as 9080. • If you configure Sterling Secure Proxy, set the port to the value defined in the Sterling Secure Proxy HTTP adapter. See "Protecting QuickFile with Sterling Secure Proxy" on page 43.

Powering off or restarting QuickFile

Use these instructions in to restart or power off QuickFile.

Before you begin

When possible, alert users in advance when you plan to restart or shut down QuickFile.

About this task

For maintenance or other purposes, you might be required to restart QuickFile or power it off. Administration gives you the ability to accomplish this task in an orderly fashion. When possible, ensure that users are notified before you power

down the server. Give users time to prepare for the temporary lack of access and to prevent file transfers from being affected.

To power off or restart the appliance, take the following steps:

Procedure

1. Click **Configuration** from the menu.
2. Click the **Power** tab.
3. To restart QuickFile, click **Restart the appliance**.
4. To shut down QuickFile, click **Power off the appliance**. If you power off the appliance, you must restart QuickFile using the VMware vSphere client.

Use LDAP to manage users and passwords

Use QuickFile with your company lightweight directory access protocol (LDAP) server. It simplifies the tasks of adding and deleting users. Using LDAP user definitions better integrates the user experience of QuickFile into their workflow.

LDAP is an industry-standard Internet Protocol. It stores and accesses user information about a server. LDAP is widely used by email and other software programs for managing user address information.

If your company uses LDAP to manage users, you can use it to manageQuickFile users. With an LDAP connection, you can eliminate most of the need to add users or user groups to QuickFile.

If you enable LDAP, do not use QuickFile to add manage LDAP users. Use the LDAP tools instead. If a user tries to log in to QuickFile with an expired LDAP password, the user is instructed to contact the administrator. As administrator, make sure that the user resets the password in the company (LDAP) directory.

Attention: You can define users in both LDAP and through QuickFile. However, users created in LDAP cannot be managed in QuickFile and users created in QuickFile must be managed through QuickFile.

After you create a user in LDAP, request that the user login to QuickFile. The user profile is displayed when the user hovers over the picture and clicks **Profile**. Users can modify their profile, including name. This value does not have to match the one defined in LDAP. Users cannot use the product to change their password. It is changed in LDAP.

Configuring an LDAP server with QuickFile

As administrator, you can configure QuickFile to use your LDAP server. Using an LDAP server eliminates the need to add and maintain users in QuickFile. Users and password information are already created in LDAP; therefore, you do not have to re-create that information. You can define users in both LDAP and QuickFile.

Before you begin

To use SSL with LDAP, enable SSL in the LDAP configuration. Then, import the LDAP server certificate into the truststore database in QuickFile from the **Configuration** menu, on the **SSL** tab. Also, set the LDAP server port to the SSL port used by the server.

About this task

Complete the following steps to configure QuickFile to use your LDAP directory.

Procedure

1. Click **Configuration** from the menu.
2. Click the **LDAP** tab.
3. To configure the LDAP connection, click **Connection Information** > **Enable LDAP integration**, and type information in the following fields.
   a. Server name
   b. Port number
   c. Principal ID
   d. Principal Password
4. To enable Secure Sockets Layer (SSL) for user authentication, check **Enable SSL**. Be sure to import the certificate into the truststore.
5. To test that your LDAP connection entries are valid, click **Test Connection**.
6. Click **Basic Information** and provide the following information:
   a. Type the **Group Base DN** to identify the group information that is specified in the LDAP database
   b. Type the **User Base DN** to identify the user information that is specified in the LDAP database
   c. To further identify a group within the base DN group, type the information in this text field and click Enter.
7. To add LDAP groups that you want QuickFile to recognize, click **Click to add**.
8. Click **Save**.

LDAP configuration field definitions

The following definitions describe the fields on the **LDAP** tab of the QuickFile Configuration page.

Field Name	Description
Enable LDAP integration	Check this box to allow the use the LDAP server. Clear the box to disable the option. Optional. The default is cleared. If you enable LDAP integration and configure it, LDAP users can use their LDAP credentials to sign into QuickFile.
Server name	The host name or IP address of the LDAP server. It must be a valid LDAP server name in your network. (IPv6 is not supported.) Required.
Port number	Port number to use to access the LDAP server. Range of valid values is 1 - 65535. Required.
Principal ID	Fully qualified distinguished name of an LDAP user authorized to search the LDAP directory. Required.
Principal Password	Password for the principal ID. Required.
Enable SSL	Check to enable Secure Sockets Layer (SSL) security. If this option is enabled, you must import the LDAP server certificate into the QuickFile truststore. Optional.
Group Base DN	Group base distinguished name. The parent node where groups are stored in the **LDAP** field. Type the node as a fully-qualified DN (ex: OU=Users,O=IBM,C=US). Required.
User Base DN	User base distinguished name. Enter the node as a fully qualified DN (ex: OU=Users,O=IBM,C=US). Required.

Field Name	Description
Group	Click **Click to add** and define the groups that are allowed to access QuickFile. Type the group as a fully qualified DN (ex: CN=QuickFile Users, OU=Users,O=IBM,C=US). Required.
Group Search filter class	Search filter for groups. Do not modify this value unless you are instructed to do so by support. Default value: (|(objectClass=group)(objectClass=groupOfNames) (objectClass=groupOfUniqueNames)).Required.
Member attributes	Array of attribute names. Do not modify this value unless support instructs you to do.
User Search filter class	Search filter for users. Do not modify this value unless you are instructed to do so by support. Required. Default value: (|(objectClass=user)(objectClass=person) (objectClass=inetOrgPerson)(objectClass=organizationalPerson))
Email attributes	An array of email attribute names. Do not modify this value unless you are instructed to do so by support.

Setting up archiving

As administrator, you can set up QuickFile to archive all file transfer activity to ensure that a record of all activity is preserved.

Before you begin

Setting up archiving requires FileNet. It also requires that you set up an appropriate FileNet document type for the archive. Finally, obtain the URL of the CMIS service document that is used to access the archiving file system. Obtain the name of the archive top-level folder. For information, consult the FileNet documentation.

Attention: Enabling archiving might significantly effect performance.

About this task

To set up archiving, complete the following steps:

Procedure

1. From the menu, click **Configuration**.
2. Click the **Archiving** tab.
3. Check **Enable an archiving system integration**. The fields for specifying archive information are activated
4. Select FileNet as the archive provider.
5. Type the **Service document URL** for the archive file system.
6. Type the name of the user who is authorized to access the archive system.
7. Type the user password for accessing the file system.
8. Type the **Top-level archiving folder** for the file system.
9. Click **Save**. Archiving is enabled. No system restart is required.

Archiving field definitions

The following table describes the fields you define to configuring archiving on the Archiving tab of the Administration Configuration features.

Field Name	Description
Enable an archiving system integration	Check this option to enable archiving and activate the remaining fields on this page.
Archive provider	Select the database application to use to archive the files. Because FileNet is the only available provider, this field is display only.
Service document (URL)	The URL where the service document of the selected archiving system is located. Field is limited to 255 characters.
Repository ID	Repository identifier to which files and packages are archived.
Authorized username	User who is authorized to access the archive file system. Required.
Authorized password	The authorized user's password for accessing the archive file system.
Top-level archiving folder	Top-level folder where archived packages and files are stored.

Chapter 8. SSL configuration overview

QuickFile uses digital certificates to authenticate the identity of the server to a user that connects to it. SSL is a protocol for enabling secure communication sessions over an unprotected network, such as the Internet. To authenticate the server to users, obtain and check in digital certificates. Server certificates are stored in the keystore.

Certificates are used to secure communications and encrypt and decrypt data. Each certificate is made up of the public key and a private key. The public key contains the information that you send to your partner. The private key is saved at your site and confirms your identity. Always keep it secret.

As an added measure of security, obtain your certificate from a certificate authority (CA). A CA verifies all of the identity information in your certificate, then adds its signature. In an SSL transaction, your certificate is presented to each user who connects to your server. The server recognizes the signature of the CA that signs the CA root certificate. Before you begin communicating with the user, make sure that the user site has a copy of the CA root certificate. The fact that the user recognizes your CA root certificate assures the user that you are who you say you are.

If you use a certificate that is not validated by a CA, it is called a self-signed certificate. Use self-signed certificates when identity verification is not required, such as communications within your company or during product testing.

To implement SSL when the transaction uses a CA certificate, import the CA root certificate into your truststore. If necessary, send the CA root certificate to the user, to include in the user truststore. Store your private key and CA certificate in the keystore. It is available for verification when you store it in the keystore.

About SSL configuration methods

Select the method to use to configure SSL. Methods include: using a new CA certificate, an existing CA certificate, a chained certificate, or a self-signed certificate.

- If you have a CA-signed certificate that you used with another application, you can import it into QuickFile.
- If you do not have a CA-signed certificate, complete a signing request to request one. Extract the information from QuickFile and send it to the CA. After CA returns the signed certificate import it into QuickFile. Enable SSL by identifying the server certificate and turn on SSL. All future connections authenticate the server to the incoming connection.
- To use a chained certificate, complete the chained certificate configuration. Enable SSL by identifying the server certificate and turn on SSL. All future connections authenticate the server to the incoming connection.
- For a less secure method, such as when you communicate with internal users or test an application, use a self-signed certificate for SSL authentication.

How to configure SSL by creating a new CA-signed certificate

To enable SSL authentication, use one of the following methods: request a new certificate from a certificate authority (CA) or use an existing CA-signed certificate to configure SSL authentication.

Complete the following procedures to request a new certificate from a CA and then configure SSL authentication in QuickFile:

- "Adding a certificate signing request"
- "Extracting a certificate from the signing request" on page 53
- Receiving the CSR from a CA
- "Enabling or disabling SSL" on page 54
- "Selecting the certificate to use for server authentication" on page 54
- "Setting basic network configuration options" on page 41

Adding a certificate signing request

To request a CA-signed certificate, complete a signing request. Then, send the request to the CA who signs it.

About this task

Note: See the documentation of the certificate authority who signs your certificate signing request (CSR) to understand the CSR requirements. If the signing request does not meet the CA requirements, it may be rejected.

Complete the following steps to create a signing request and add it to the signed request store:

Procedure

1. Click **Configuration** from the menu.
2. Click the SSL tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the signed request store to open.
5. Click **New**. The Certificate signing request page is displayed.
6. Type the key label to use when you reference this request in the **Key Label** field.
7. Type the common name that is used to reference the company or URL that is being validated in the **Common name** field.
8. Type information in the remaining optional fields as needed.
9. Click **Create**.

New signing request field definitions

Create a signing request to create a certificate and send it to a CA to sign. The following table identifies the fields to define when creating a signing request.

Field	Description
Key Label	Label to assign to the certificate signing request you create.
Key size	Key length required for the certificate public key to validate the key.

Field	Description
Common name	Fully-qualified domain name (FQDN), host name, or URL to which you plan to apply your certificate. If the common name in the certificate does not match the value defined in this field, the session fails.
Organization	Name under which your business is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request. If you enroll as an individual, type the certificate requestor name in the Organization field. Type the DBA (doing business as) name in the Organizational Unit field.
Organizational unit	Define this field to differentiate between divisions within an organization. For example, "Engineering" or "Human Resources." If applicable, type the DBA (doing business as) name in this field.
Locality	Name of the city in which your organization is registered or located. Spell out the name of the city. Do not abbreviate.
State/Providence	Name of the state or province where your organization is located. Type the full name. Do not abbreviate.
Postal Code	Postal code for the city in which your organization is located.
Country or region	Two-letter International Organization for Standardization (ISO) format country code for the country in which your organization is legally registered.

Extracting a certificate from the signing request

After you create a signing request, extract the certificate and send the information to the certificate authority (CA).

About this task

Complete the following steps to extract the certificate from the signing request. You can then send it to the CA.

Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the signing request store where the CSR is stored.
5. Select the signing request to extract and click **Extract**.
6. Copy the text from the dialog and paste it into another file. Save the file.
7. Click **Close**.
8. Send the file to your CA and request that it is signed and returned to you.

Uploading a keyfile received from a CA

Use this procedure to upload a keyfile received from a CA.

About this task

To upload a key file from a CA:

Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the keystore to open.
5. Click **Upload key file**.
6. Enable **Import from a keyfile** and click **Browse** to locate the file.
7. Click **Upload**.

Enabling or disabling SSL

After you configure your certificates and check them into the database, you then enable SSL. If you want to turn off SSL authentication, use this procedure.

Procedure

1. Click **Configuration**.
2. Click the **SSL** tab.
3. If necessary, click **Configuration** to view the SSL configuration options.
4. Turn on **Enable secure connections (SSL)**.
5. To disable SSL, turn off **Enable secure connections (SSL)**.
6. Click **Save**. Restart your browser to activate the changes you made.

Selecting the certificate to use for server authentication

This procedure identifies the certificate used to authenticate the server. If certificates change, change the certificate setup.

Before you begin

To enable the certificate to use to authenticate the server to users who connect to the application:

Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Select the certificate to use for authentication in the **Server certificate** field.
4. Click **Save**.

How to configure SSL by using an existing CA-signed certificate

To enable SSL authentication, use one of the following methods. Request a new certificate from a certificate authority (CA), generate and use a chained certificate, or use an existing CA-signed certificate to configure SSL authentication.

Complete the following procedures to use an existing CA-signed certificate to authenticate a connection and configure QuickFile to be authenticated by incoming connections:

- "Uploading a key file and importing a certificate"
- "Enabling or disabling SSL" on page 54
- "Selecting the certificate to use for server authentication" on page 54
- "Setting basic network configuration options" on page 41

Uploading a key file and importing a certificate

To authenticate the QuickFile server with a certificate that you obtained from a CA, upload the CA key file into the database.

About this task

To upload a key file:

Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the keystore where the certificate is imported.
5. Click **Upload key file**. The Upload key files dialog is displayed.
6. Enable **Import from a keyfile** and click **Browse** to locate the file.
7. Click **Upload**. The **Import Certificate** page is displayed.
8. Type information about the certificate, including key file name and password and imported certificate alias.
9. Click **Import**.

How to configure SSL with a chained certificate

To enable SSL authentication with a chained certificate, create a chained certificate and sign it with a root CA certificate. Then, you are ready to enable security with the chained certificate.

Complete the following procedures to create a new chained certificate and configure SSL authentication in QuickFile:

- "Configuring chained certificates" on page 56
- "Enabling or disabling SSL" on page 54
- "Selecting the certificate to use for server authentication" on page 54
- "Setting basic network configuration options" on page 41

About chained certificates

To increase security, you can use CA certificate chaining.

In certificate chaining, two or more CA certificates are linked in a certificate chain. The primary CA certificate is the root certificate at the end of the CA certificate chain. It must be present in order to verify the authenticity of a certificate that is received. A certificate chain can be stored in a single file, such as a .pem file. It can be stored in separate files. , where each file contains one CA certificate in the chain. If you intend to use certificate chaining, ensure that each CA certificate in the chain is installed in the truststore.

Configuring chained certificates

To increase security, use a chained CA certificate. Before you create a chained certificate, import the key of the root certificate into the truststore. The root certificate is used to sign the chained certificate.

About this task

To configure a chained certificate, complete the following steps:

Procedure

1. Click **Configuration** on the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the keystore to open.
5. Click **Create > Chained certificate**. The Create chained certificate page is displayed.
6. Type the alias that is used for this certificate in the **Alias** field.
7. Select the root certificate that is used to sign the certificate.
8. Type the common name to use for the chained certificate.
9. Select the key size of the root certificate from the list.
10. Type the common name to use for the chained certificate.
11. Type how many days the certificate is valid in the **Validity period** field.
12. If needed, type information about the server to validate in the remaining fields.
13. Click **Create**.

Chained certificate field definitions

When you receive the certificate for another entity, you might need to use a certificate chain to obtain the root CA certificate. The certificate chain is a list of certificates that are used to authenticate an entity. The chain begins with the certificate of that entity. Each certificate in the chain is signed by the entity that is identified by the next certificate in the chain. The chain terminates with a root CA certificate. The root CA certificate is always signed by the CA itself. The signatures of all certificates in the chain must be verified until the root CA certificate is reached. The following table identifies the fields that you define when you configure a chained certificate in QuickFile.

Field	Description
Alias	The alias that is associated with the certificate. The secure listener and connection definitions that specify SSL use the alias to reference the certificate.
Root certificate used to sign the certificate	The name of the root certificate. If the request does not include the complete certificate chain, the truststore is searched for the issuer certificates.
Key size	Size of the key that is used to sign the certificate. Available values are: 512, 1024, and 2048. Most certificate providers are moving to 2048-bit key sizes.

Field	Description
Common name	Fully qualified domain name (FQDN), host name, or URL to which you plan to apply your certificate. If the common name in the certificate does not match the value that is defined in this field, the session fails.
Validity period	How long the certificate can be used for authentication. Type the number of days, up to 356 days.
Organization	Name under which your business is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request. If you enroll as an individual, type the certificate requestor name in the **Organization** field. Type the DBA (doing business as) name in the **Organizational Unit** field.
Organization Unit	Define this field to differentiate between divisions within an organization. For example, "Engineering" or "Human Resources." If applicable, type the DBA (doing business as) name in this field.
Locality	Name of the city in which your organization is registered or located. Spell out the name of the city. Do not abbreviate.
State/Providence	Name of the state or province where your organization is located. Type the full name. Do not abbreviate.
Postal Code	Postal code for the city in which your organization is located.
Country or region	The two-letter International Organization for Standardization (ISO) format country code for the country in which your organization is legally registered.

How to configure SSL by using a self-signed certificate

To enable SSL authentication by using a self-signed certificate, you create a self-signed certificate.

Complete the following procedures to create a self-signed certificate and configure SSL authentication in QuickFile:

- “Creating a self-signed certificate”
- “Enabling or disabling SSL” on page 54
- “Selecting the certificate to use for server authentication” on page 54
- “Setting basic network configuration options” on page 41

Creating a self-signed certificate

For a quick way to test your environment, use a self-signed certificate. It is not signed by a CA and does not provide the security that is required in a production environment. If you use a self-signed certificate to test your environment, be sure to replace it before you use the product.

About this task

To configure a self-signed certificate, complete the following steps:

Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the keystore to open.
5. Click **Create > Self-signed certificate**. The Create Self-signed Certificate page is displayed.
6. Type the alias to use for this certificate in the **Alias** field.
7. Select the common name that is identified in the certificate in the **Common name** field.
8. Type how many days the certificate is valid in the **Validity period** field.
9. If wanted, type information about the server in the remaining fields.
10. Click **Create**.

Self-signed certificate fields

Create a self-signed certificate to enable SSL for an internal environment. A self-signed certificate is not as secure as using a CA certificate. However, it provides a level of security that can be used for testing and for validating the server to users inside the enterprise.

Field	Description
Alias	The alias that is associated with the certificate. The secure listener and connection definitions that specify SSL use the alias to reference the certificate.
Version	Version that is used to create the self-signed certificate: X509v3 or IBMX509
Key size	Key length that is required for the public key to validate the certificate.
Common name	Fully qualified domain name (FQDN), host name, or URL to which you plan to apply your certificate. If the common name in the certificate does not match the value that is defined in this field, the session fails.
Validity period	How long the certificate can be used for authentication. Type the number of days, up to 356 days.
Organization	Name under which your business is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request. If you enroll as an individual, type the certificate requestor name in the **Organization** field. Type the DBA (doing business as) name in the **Organizational Unit** field.

Field	Description
Organization Unit	Define this field to differentiate between divisions within an organization. For example, "Engineering" or "Human Resources." If applicable, type the DBA (doing business as) name in this field.
Locality	Name of the city in which your organization is registered or located. Spell out the name of the city. Do not abbreviate.
State/Providence	Name of the state or province where your organization is located. Type the full name. Do not abbreviate.
Postal Code	Postal code for the city in which your organization is located.
Country or region	The two-letter International Organization for Standardization (ISO) format country code for the country in which your organization is legally registered.

Importing a certificate into the keystore

Use this procedure to specify a personal certificate to import from a keystore or key file. Upload the keyfile before you import a certificate.

About this task

To import a certificate into the keystore:

Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to view the keystore and truststore.
4. Click **More>Import**. The **Import Certificate** page is displayed.
5. Type information in the following required fields:
   - Key file name
   - Key file password
   - Imported certificate alias
6. Click **Import**.

Import Certificate field definitions

When you import a key file from a file, use the fields in the following table to import the certificate:

Field	Description
Key file name	Name of the key file that contains the public key and the private key.
Type	Select the type of key to import: JKS or PKCS12
Key file password	The password that locks the key file and is used to import the certificate.

Field	Description
Get keyfile aliases	Click the button to query the key file for the aliases of all the personal certificates in the keystore.
Certificate alias to import	Certificate alias identified as the key file name that you want to import into the current keystore.
Imported certificate alias	New alias that you want the certificate to be named in the current keystore.

Uploading a certificate file for storage

Use this procedure to upload a file into the keystore. The file is not available to use with application. It is only stored for future use.

About this task

To upload a certificate file for storage, complete the following procedure:

Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.
3. Click **Certificate Management** to expand the section.
4. Click the name of the keystore where the file is uploaded.
5. Click **Upload key file**. The Upload key file page is displayed.
6. Enable **Just upload the file** and click **Browse** to locate the file.
7. Click **Upload**.

Upload key file field definitions

Use the Upload key file window to define how to upload files into the keystore or from files that are received from a CA. The fields are described in the table.

Field	Definition
Attach file to upload	Either drag the keyfile to upload to the Attach box or Browse to select the keyfile.
Select what you want to do with the file	Select the action to take with the file you are uploading: Receive from CA, Import from a keyfile, or upload the file.

Deleting a certificate from the keystore

Use this procedure to delete a certificate from the keystore.

About this task

To delete a certificate from the keystore:

Procedure

1. Click **Configuration** from the menu.
2. Click the **SSL** tab.

3. Click the name of the keystore that contains the certificate to delete.
4. Click the certificate to delete.
5. Click **More>Delete**. The Delete Certificate page is displayed.
6. Click **Delete**.

Chapter 9. Viewing a log of system events

As administrator, you can view a log of the events that are generated by QuickFile.

About this task

You can view a log of events that are generated by QuickFile. You determine the number of events to display per page and sort the listing by event type or date. By default, events are sorted first by date and time and next by event name.

To view system events:

Procedure

1. Click **Log reports** from the menu.
2. Make sure that the **System logs** tab is selected.
3. To sort the event list by event or event date, click the appropriate heading.
4. If more than one page of events is available in a report, click **Next** to display the next page in a report.
5. To move back to a previous page in the events report, click **Previous** .
6. To view the last page of events, click the last page number in the **Page** listing.
7. To view the first page of events, click the first page number in the **Page** listing.
8. To jump to a specific page, type the page number in the **Jump to page** text box or click the page number in the **Page** listing.

Event log explanation

System events can be viewed by administrators only and describe the events that occur in QuickFile. Each message uses the code format CIVxx*nnnn*T, where *nnnn* is a unique message number and *T* is the message type. Refer to the following tables for a description of the message code components and the messages that occur:

Message Code Component	Description
xx	The message code prefix. Available prefixes include: • ST - storage • ID - identity • MB - mailbox • VI - visibility • MS - messaging • CF - configuration • CN - communication • SC - scheduling • CC - common components
T	Message type. Available message types include: • E = error • I = information • W = warning

The following table identifies the messages created in QuickFile. It identifies the category of event, the event code assigned to the message, the message text, and an explanation.

Event	Event Code	Message	Description
Self registered	CIVID1001I	<user> self registered	A user completed the registration form from the login page. The user must click a link in the registration email to complete the process.
Register Confirmed	CIVID1006I	<user> confirmed registration	A user clicked a link in the registration email to complete the registration.
Registration Expired	CIVID1002I	<user> self registration expired	A user completed the registration form from the login page but did not click a link in the registration email to complete the process.
User Created	CIVID1005I	<user> created by administrator	An administrator added a user. The user must click a link in an email to complete the user registration.
Unlocked	CIVID1014I	<user> unlocked by administrator	Administrator unlocked the user.
User Deleted	CIVID1016I	<user> deleted by administrator	User was deleted from the database by the administrator. **Note:** User records are never removed from the database. They are marked as deleted and the user is prevented from logging in.
Login	CIVID1007I	<user> logged in	User is logged in.
Failed due to locked	CIVID1015I	<user> locked; repeated login failures	User is unable to log in because the user exceeded the maximum number of failed login attempts set by the administrator.
Logout	CIVID1008I	<user> logged out	User is logged out.
Sent	CIVCC1001I	<user1> sent file <f> in package <p> to <user2>	A user sent a file called *f* to another user. The file is saved to the server. User 2 can now download the file.
Downloaded	CIVCC1004I	<User> downloaded a file <f`>	A user downloaded a file called *f*.
Deleted	CIVID1016I	<user> deleted file <f`> with package <p>	User deleted a file from the file listing. The file is stored on the server and is marked for removal.
Sent	CIVCC1014W	Upload failed because <file1> with package subject exceeds required limit	The file that the user sent is larger than the file size limit and is not transferred.
File Archived	CIVCC1011I	<files> in <package> for <user> were archived	Files for a user were archived.
Expiration changed	CIVCC1021I	User updated expiration date of a file with package subject	A user updated the expiration date of a file in a package
Re-sent	CIVCC1002I	<user1> resent file <f> with package subject <p> to <user 2>	User 1 resent a file called *f* to user 2. The file is sent to the same user who received the file on the first transfer. The file is saved on the server. The user can now download the file.
Forwarded	CIVCC1003I	<user1> forwarded file <f`> with package subject <p> to <user 2>	User 1 forwarded a package called *p* to a new user 2. The file is saved on the server. The user can now download the file.
Invited	CIVID1003I	<user1> invited <user2> to register	User1 sent an invitation to another user to register. To complete the invitation, user 2 must click a link in the email to complete the process.

The following table identifies the messages created in QuickFile. It identifies the category of event, the event code assigned to the message, the message text, and an explanation.

Event	Event Code	Message	Description
Requested	CIVCC1005I	<user1> requested <user2> to send file with package subject	A user sent a request to another user to send a file.
Password Change	CIVID1009I	<user> changed password	User 1 changed their password.
Password Forgotten		<user> forgot password	User forgot the password and requested a temporary one.
Password Failed	CIVID1010I	<user> failed to login; forgot password	User 1 was unable to log in because the user provided an invalid password.
AFT Enabled	CIVID1011I	<user> enabled Advanced File Transfer	User enabled the Advanced File Transfer option to allow the transfer of large files and to enable pause and resume.
AFT Disable	CIVID1012I	<user> disabled Advanced File Transfer	User disabled the Advanced File Transfer option.
AFT Uploaded	CIVCC1012I	<user1> uploaded <n> out of <n> bytes of <file> with package subject <p> to <user2>	User used Advanced File Transfer to send a portion of a file as identified in the <n> out of <n> bytes definition. File is sent to user 2.
AFT Downloaded	CIVCC1013I	<user1> downloaded <n> out of <n> bytes of <file> with package subject <p> to <user2>	User used Advanced File Transfer to download a portion of a file identified in the <n> out of <n> bytes definition. File is sent to user 2.
User Locked	CIVID1013I	<user> locked by administrator	User is unable to log in to QuickFile because the administrator locked out the user.
Profile Updated	CIVID1017E	<user> updated profile	User modified the profile.
Group Created	CIVID1021I	<group> created by administrator	The administrator created a group.
User Added to Group	CIVID1018I	<user> was added to <groupn> by administrator	The administrator added user 1 to a group definition. The group definition determines the policy that is enforced for all users in the group.
User Removed from Group	CIVID1019E	<user> was removed from <groupn> by administrator	The administrator removed user 1 from the group definition. User policy enforced when a user is not part of a group are the default settings.
Role Modified	CIVID1020I	<user> assigned the role of <administrator or user> by administrator	The administrator modified the role of the user identified. Available roles include user or administrator.
Group Modified	CIVID1023I	<group> modified by administrator	The administrator modified the group.
Group Deleted	CIVID1022I	<group> deleted by administrator	The administrator deleted the group called <group>.
Powering Down	CIVCF1003I	<administrator> powering down the appliance	The appliance is powering down.
Powered Down	CIVCF1001I	<administrator> powered down the server	An administrator is shutting down the server.
Appliance Restarted	CIVCF1002I	<administrator> restarting the appliance	An administrator restarts the server.

The following table identifies the messages created in QuickFile. It identifies the category of event, the event code assigned to the message, the message text, and an explanation.

Event	Event Code	Message	Description
Server Started	CIVCF1004I	The server was started	An administrator started the server.
NFS Configured	CIVCF1005I	Application is configured to use NFS with <nfs configuration>	The application is using NFS.
Database Configured	CIVCF1006I	Application is configured to use external database with <db configuration>	The application is using the external database.
LDAP Configured	CIVCF1007I	Application is configured to use external directory with <LDAP configuration>	The application is using LDAP.
Archive Configured	CIVCF1008I	Application is configured to archive using <Filenet configuration>	The application is using FileNet to archive files.
SMTP Configured	CIVCF1009I	Application is configured to use the SMTP server with <SMTP configuration>	The application is using an SMTP server.
SMTP Server Failed	CIVCF1028E	Failed to connect to the SMTP server	The application failed to connect to the SMTP server.
No SMTP Server	CIVCF1027E	No SMTP server configured	No SMTP server is configured.
SMTP Failed	CIVCF1025E	SMTP server connection failed.	The SMTP server connection failed.
IP Configured	CIVCF1011I	Application is configured to use IP address with <ip address>	The application is using an IP address.
Gateway Configured	CIVCF1012I	Application is configured to use Gateway server with <gateway configuration>	The application is using a Gateway server.
Mask Configured	CIVCF1013I	Application is configured to use subnet mask with <CIDR mask configuration>	The application is using a subnet mask.
NFS Connection Failed	CIVCF1020E	NFS with <nfs configuration> failed to connect	NFS did not successfully connect to the server.
DNS Connection Failed	CIVCF1024E	The Gateway server using the <gateway configuration> failed to connect	The gateway server did not successfully connect.
Database Connection Failed	CIVCF1021E	External database with <db configuration> failed to connect	The external database did not successfully connect to the server.
LDAP Connection Failed	CIVCF1022E	LDAP with <ldap configuration> failed to connect	LDAP did not successfully connect to the server.
Archive Connection Failed	CIVCF1023E	Archive with <archive configuration> failed to connect	The archive tool did not successfully connect to the server.
Fix Pack Failed	CIVCF1026E	Fix pack updates with <update info> failed	The fix pack did not successfully install.

The following table identifies the messages created in QuickFile. It identifies the category of event, the event code assigned to the message, the message text, and an explanation.

Event	Event Code	Message	Description
Out of Disk Space	CIVCF1029E	Appliance ran out of disk space	The appliance ran out of disk space and therefore, packages can no longer be uploaded.
SSL Expired	CIVSE1001I	SSL certificate <alias> expired	The SSL certificate expired. Request a new one from your CA.
SSL Imported	CIVSE1002I	SSL certificate <alias> imported by administration	The administrator imported an SSL certificate.
SSL Exported	CIVSE1003I	SSL certificate <alias> exported by administration	The administrator exported an SSL certificate.
SSL Disabled	CIVSE1005I	SSL disabled	The administrator disabled SSL.
SSL Enabled	CIVSE1004I	SSL enabled	The administrator enabled SSL.
Status Updated		Users: registered <#>, unregistered <#>, active <#>; Storage; used <used> available <available>; number of files <# of files>; users: registered <registered #> unregistered <unregistered #> active <active #>	The status information is updated.
File Removed	CIVCC1010I	<files> in <package> for <user> were abandoned after 7 days and will be removed	The package identified was paused and was not restarted before 7 days elapsed. The package is marked for deletion.
File Archived	CIVCC1011I	<files> in <package> for <user> were archived.	Files for a user were archived.

Generating a support log

If support instructs you to generate a support log, use QuickFile to generate a support log.

About this task

When troubleshooting a problem you experience with QuickFile, support might ask you to turn on the support log. QuickFile makes this job easier with Log Reports.

One of the Log Reports tabs gives you the ability to turn on the support log. Using the support log, you can generate logging information and export the information to a file for support to use. Because of the temporary impact that logging has on system performance, turn on logging only when support instructs you to do so.

To turn on logging, complete the following procedure:

Procedure

1. Click **Log reports** from the menu.
2. Click the **Support logs** tab.
3. Turn on **Enable support logging**.
4. Select one of the following application logs to view:

- Application server
- Database
- Messaging
- Operating system

5. If you select Application server as the log to view, type the exact log information as instructed by support.
6. If you select database, provide information in the following fields:
   - Log severity Level
   - Log query plan
   - Log statement text
   - Deadlock trace
7. If you select Messaging as the log type, select one or more of the following fields to define the log levels to view:
   - cluster
   - dap
   - defs
   - kernel
   - logger
   - topic
   - trace
8. If you select Operating system, select one of the following error levels to log:
   - Debug
   - Info
   - Warn
   - Error
   - Message
   - Fatal
9. To export the event log to a file, complete the following steps:
   - Select the dump files to export, enable Java dump files or heap dump files or both.
   - Click **Export**. A file is downloaded to your computer.
   - Open or save the file as needed.
10. Click **Save**.
11. Under direction from support, re-create the original problem. After you recreate the problem, return to this page.
12. Send the log files to support for analysis.

Viewing events that are not in the log

You can use the event log to generate a list of commonly occurring tasks. However, not all events and errors are available in the log. Use the information in this topic to gather and download all the system logs.

Before you begin

Complete the following steps to gather and download all system logs:

Procedure

1. Type the following url in your browser: `http://`*ip address*`:9080/quickfile/rest/admin/mustgather`.
2. Type your administrator user ID and password.
3. Save the file called `quickfileMustGather.tgz`.
4. Unzip the file to view all QuickFile logs.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2014. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2014.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise®, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce®, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

Index

M

N

O

P

Q

R

S

T

U

V

Product Number: 5725-F81

Printed in USA